4/2012

Datenschutz Nachrichten

35. Jahrgang
ISSN 0137-7767
9,00 Euro

Datenschutzgerechte Webseiten

■ Unbefriedigende Datenschutzkompromisse ■ Do Not Track: Zum Konflikt zwischen Microsoft und der US-Wirtschaft ■ Wir speichern nicht ■ Datenschutz-Tools für den Besuch von Internetseiten ■ Haken und Ösen bei der Verwendung von Mitarbeiterfotos durch den Arbeitgeber ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Montag, 31.12.2012
BigBrotherAwards 2013
Einsendeschluss für Nominierungen
https://www.bigbrotherawards.de/nominate

Freitag, 1. Februar 2013
Redaktionsschluss DANA 1/13
Thema: „Löschen“
verantwortlich: Karin Schuler

Samstag, 26. Januar 2013, 10:00 Uhr
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 12. April 2013, 12:00 Uhr
DVD-Vorstandssitzung
Bielefeld. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 12. April 2013, 18:00 Uhr
Verleihung der BigBrotherAwards 2013
Bielefeld
http://www.bigbrotherawards.de

Mittwoch, 1. Mai 2013
Redaktionsschluss DANA 2/13
Thema: N.N.

Montag, 17. Juni 2013 und Dienstag, 18. Juni 2013
DuD 2013 – 15. Jahresfachkonferenz
Datenschutz und Datensicherheit
Berlin.
http://www.computas.de/konferenzen/dud_2013/DuD_2013.html

Sonntag, 28. Juli 2013, 10:00 Uhr
DVD-Vorstandssitzung
Berlin. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
35. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Frans Jozef Valenta
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Screenshots
Frans Jozef Valenta

Editorial

Liebe Leserinnen und Leser,

vor einigen Tagen wurde über ein Ereignis berichtet, dass sehr deutlich die Problematik des Leitthemas dieses Heftes verdeutlicht: Als Sumit Summan die Webseite des Webmarketing-Dienstleisters uberVu.com besuchte, trug er keine persönlichen Daten ein und verknüpfte sich auch nicht mit den Social-Media-Angeboten der Firma. Daher wunderte er sich, dass er am nächsten Tag Werbeangebote per E-Mail von dieser US-Firma bekam. Hierüber verfasste er einen Google+-Beitrag und erhielt eine Entschuldigung der Community-Managerin von uberVu mit der Zusicherung, dass keine weiteren Werbemails mehr an ihn verschickt würden. Es stellte sich heraus, dass die Identifizierung über die Technologie der Firma LeadLander erfolgte, die offensichtlich in der Lage war, Besucher durch Geodaten und den Abgleich mit sozialen Netzwerken zu bestimmen.
Die Scripte zur Identifikation von Webseitenbesuchern verrichten ihre Aufgaben immer präziser. Das Titelbild (schwarzer Bereich) gibt einen Eindruck von der Kompexität der Programmierung. Der hier zum Teil abgebildete Code wurde der Internetseite einer großen deutschen Tageszeitung entnommen.
Eines der Tools zur Erforschung des Nutzerverhaltens im Internet ist Google Analytics. Michael Knopp befasst sich in seinem Artikel um die Aspekte einer rechtskonformen Verwendung.
Zu einem datenschutzfreundlichen Internet gehört auch die Möglichkeit zur Unterbindung von Tracking. Microsoft hat eine entsprechende Funktion im Internet Explorer 10 vorgesehen – das Unternehmen und die Nutzer stoßen bei der Diskussion um einen Do-not-Track-Standard allerdings auf massiven Widerstand der Industrie. Mehr darüber erfahren Sie im Artikel von Kirsten Bock.
Wer sich unbehelligt von Tracking und Scripting im Web umsehen möchte, werfe einen Blick auf „Nützliche Datenschutz-Tools für den Besuch von Internetseiten“.

Frans Jozef Valenta

Autorinnen und Autoren dieser Ausgabe:

Kirsten Bock
Referatsleiterin EuroPriSe beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. kbock@datenschutzzentrum.de

Michael Knopp
Jurist und Consultant bei Secorvo Security Consulting GmbH.
michael.knopp@secorvo.de

Robert Malte Ruhland
Rechtsanwalt, Sachverständiger für Datenschutz, Compliance-Beauftragter und externer Datenschutzbeauftragter in Dortmund. Rechtsanwaltskanzlei Ruhland, Ruhrallee 9, 44139 Dortmund, fon 0231 98 18 970, info@kanzlei-ruhland.de, www.kanzlei-ruhland.de

Jens Seipenbusch
Stellvertretender Leiter der Informationsverarbeitungs-Versorgungseinheit (IVV) der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster. Mitarbeit im Arbeitskreis Vorratsdatenspeicherung. jens.seipenbusch@gmx.de

Frans Jozef Valenta
Selbständiger Grafik Designer und Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz. valenta@t-online.de

Michael Knopp

Unbefriedigende Datenschutzkompromisse

Google-Dienste, Tranzparenzanforderungen und rechtliche Grenzen aufsichtsbehördlichen Entgegenkommens

1 Die Google-Welt und der Datenschutz

Wollte man aktuelle und künftige Bedrohungen der informationellen Selbstbestimmung außerhalb staatlicher Datenerhebungen sammeln, ist Google eine Adresse, an der man nicht vorbei kommt. Google ist praktisch der Maßstab für das Funktionieren der datenschutzrechtlichen Regulierung elektronischer Kommunikation.



Unter dem Dach der Google Inc. sind die führende Internet-Suchmaschine, mit Youtube eine führende Videoplattform, mit Google+ ein soziales Netzwerk, mit Google Analytics ein verbreiteter Tracking-Dienst zur Analyse des Nutzerverhaltens, mit Google-Mail ein Provider von E-Mail-Diensten, mit Google Docs cloud-basierte Officesoftware und mit Google Kalender ein Cloud-Terminplaner vereint, um nur die wichtigsten und bekanntesten Dienste zu nennen. Mit Google Streetview, Google Earth und -Maps, dem Google-Browser Chrome und vor allem durch die Verbindung zu dem Smartphone-Betriebssystem Android, das ohne Google-Nutzerkonto praktisch nicht vollständig genutzt werden kann, wird die Reichweite der Google-Dienste noch weiter vergrößert. Das Google-Nutzerkonto, ohne das ein Teil der Dienste nicht genutzt werden kann, steht als Klammer über den verschiedenen Diensten.

Bereits einzeln bieten die Nutzungsdaten aus diesen Diensten ein enormes Potenzial zur Bildung von Persönlichkeitsprofilen. Zusammengeführt und personenbezogen lassen sich der Umfang und die Aussagekraft kaum noch einschätzen. Für den Nutzer handelt es sich um kostenfreie Dienste, tatsächlich jedoch sind seine Daten die Grundlage von Googles Geschäftsmodell, was Google eifrig als risikolos und nur vorteilhaft zu verkaufen bestrebt ist.

Umso wichtiger erscheint, dass die Datenverarbeitung eines solchen Unternehmens für den Nutzer transparent gestaltet wird, dass Aufsichtsbehörden sich von der Einhaltung rechtlicher Verarbeitungsgrenzen bezüglich der von Ihnen geschützten Personenkreise überzeugen können und dass klare Regeln bestehen und respektiert werden, die diese Grenzen festlegen.

Hiervon ist die Realität noch weit entfernt. Das zeigt sich zum einen an den aktuellen Entwicklungen in Sachen Datenschutzerklärungen und Nutzungsbedingungen, zum anderen an dem Stand zu Google Analytics.

2 Google Nutzungsbestimmungen und Datenschutzerklärung

Am 1.3.2012 hat Google mit einer Überarbeitung seiner Nutzungsbedingungen und Datenschutzerklärungen für Aufregung gesorgt.[1] Über 60 Datenschutzerklärungen zu einzelnen Diensten wurden zu einer zentralen Erklärung mit verschiedenen Ergänzungen zusammengefasst. Die früheren Datenschutzerklärungen sind nicht mehr verfügbar. Inzwischen liegt eine geänderte Version vom 27.7.2012 vor, die jedoch in Bezug auf die datenschutzrechtlich entscheidenden Aussagen keine Änderungen enthält.[2]

2.1 Inhalte der Datenschutzerklärungen

Kern der neuen Datenschutzerklärung sind die Aussagen „Wir verwenden den von Ihnen für Ihr Google-Profil angegebenen Namen möglicherweise für alle von uns angebotenen Dienste, die ein Google-Konto erfordern. Darüber hinaus ersetzen wir möglicherweise Namen, die in der Vergangenheit mit Ihrem Google-Konto verknüpft waren, damit Sie in all unseren Diensten einheitlich geführt werden. Wenn andere Nutzer bereits über Ihre E-Mail-Adresse oder andere Sie identifizierende Daten verfügen, werden wir diesen Nutzern gegebenenfalls die öffentlich zugänglichen Informationen Ihres Google-Profils, wie beispielsweise Ihren Namen und Ihr Foto, anzeigen.“ und „Unter Umständen verknüpfen wir personenbezogene Daten aus einem Dienst mit Informationen und personenbezogenen

Daten aus anderen Google-Diensten. Dadurch vereinfachen wir Ihnen beispielsweise das Teilen von Inhalten mit Freunden und Bekannten.“ Als weiterer Zweck wird angegeben, die erhobenen Informationen zur Bereitstellung, zur Instandhaltung, zum Schutz sowie zur Verbesserung der Google-Dienste, zur Entwicklung neuer Dienste sowie zum Schutz von Google und seiner Nutzer zu verwenden. Weiter wird ausgeführt, dass die Informationen für das Anbieten maßgeschneiderter Inhalte und das zur Verfügung stellen relevanter Suchergebnisse und Werbung genutzt werden.

Begriffe wie „möglicherweise“, „gegebenenfalls“ und „unter Umständen“ werden in der Datenschutzerklärung bei vielen Aussagen zur Datenverarbeitung verwendet. Auch die Nutzungsbedingungen enthalten unbestimmte Begriffe wie „einige“, „unter Umständen“, „kann“, auch in Bezug auf datenschutzrechtlich relevante Aussagen. Die Nutzungsbedingungen gehen ferner von einer Einwilligung durch Nutzung der Dienste in die Verarbeitung personenbezogener Daten gemäß der Datenschutzbestimmungen aus. Bei Eröffnung eines Google-Kontos wiederum wird eine Bestätigung der verlinkten Nutzungsbedingungen und der Datenschutzerklärung eingeholt, wobei die Einwilligung in die Verwendung der Kontoinformationen zur Anzeige personalisierter Google+ Empfehlungen auf den Webseiten Dritter bereits voreingestellt ist.[3]

Die Datenschutzerklärungen werden ergänzt durch „Datenschutzprinzipien“, in denen weitere Angaben niedergelegt werden. Beispielsweise die Beteuerung, keine Nutzerdaten zu verkaufen oder kontinuierlich in Kooperation mit Behörden und Branchenpartnern an der Implementierung hoher Datenschutzstandards zu arbeiten.[4] Übereinstimmend mit der zentralen Datenschutzerklärung wird auf das Dashboard mit Einstellungsmöglichkeiten zur Datenverarbeitung und Datenschutztools als Mittel der Transparenz und zur Selbstbestimmung verwiesen. Die Tools enthalten unter anderem Einstellungsmöglichkeiten des Google-Browsers Chrome zur Beendigung der Verlaufsaufzeichnung, zur verschlüsselten Übermittlung von Google-Suchanfragen sowie -ergebnissen, Deaktivierungsmöglichkeiten bezüglich personalisierter Werbung, Antragsformulare zur Unkenntlichmachung von Objekten in Google Streetview und zur Vornahme von Veröffentlichungsbeschränkungen bezüglich personenbezogener Daten, die der Nutzer über Google Dienste teilt.[5] Weiter existieren neben den Datenschutzerklärungen Informationsseiten mit Erläuterungen. Hier wird vereinzelt deutlich detaillierter erklärt, welche Daten Google etwa bei Suchanfragen speichert und wie diese genutzt werden.[6] Beispielsweise finden sich hier klare Angaben zur Speicherdauer der IP-Adresse und zur Verwendungsdauer der Identifizierungs-Cookies.[7]

Sämtliche Erklärungen betonen vielfach, dass Google keine Daten erhält, die zu einer Identifizierung des Betroffenen führen. Ebenso wird versichert, dass keine Verknüpfung von Cookies oder Kennungen mit sensiblen personenbezogenen Daten erfolgt oder dass keine Weitergabe von personenbezogenen Daten an Dritte erfolgt, außer an Auftragsdatenverarbeiter, nach Erteilung einer Einwilligung oder an Konto-Administratoren.

Ergänzende Einzelbestimmungen folgen zu den Diensten Google Wallet, Google Books und zu dem Browser Chrome. Die Datenschutzerklärung zu dem Bezahldienst Wallet arbeitet bezüglich der Weitergabe von personenbezogenen Daten zu Werbezwecken an Dritte mit dem Angebot eines Opt-out.[8]

Die Verknüpfung dieser unterschiedlichen Informationsquellen zur Datenverwendung untereinander ist äußerst unübersichtlich, da sie teilweise gar nicht oder nur einseitig aufeinander Bezug nehmen. Eine Auflistung sämtlicher in Kraft befindlicher Datenschutzerklärungen, datenschutzrelevanter Erläuterungen und Einstellungen ist nicht vorhanden. Das Ziel, durch eine einheitliche Erklärung die Transparenz zu erhöhen, wird daher verfehlt. Da die zusammengefasste Datenschutzerklärung zudem bezüglich der Verwendungszwecke der Daten nicht nach Daten und Diensten differenziert, fehlt auch eine systematische Übersicht über wesentliche Informationen.

2.2 Feststellungen der Art. 29 Gruppe

Die oben beschriebenen Nutzungsbestimmungen und Datenschutzerklärungen sind von der französischen Datenschutzaufsichtsbehörde Commission Nationale de l'Information et des Libertés (CNIL) im Auftrag der Art. 29 Gruppe der Europäischen Union untersucht worden. Auf Grundlage der Ergebnisse[9] haben die Mitglieder der Art. 29 Gruppe ein gemeinsames Schreiben mit Schlussfolgerungen an Google Inc. gerichtet.[10]

In diesem Schreiben wird beanstandet, dass die Erklärung in keiner Weise die Einhaltung der Datenschutzgrundprinzipien Datensparsamkeit, Zweckbindung, Erforderlichkeit sowie die Gewährung eines Widerspruchsrechts gewährleistet. Im Gegenteil seien keine Begrenzungen der Datenerhebung und der Verarbeitungszwecke erkennbar.

Besonderes kritisch wird die diensteübergreifende Zusammenführung und Auswertung der Nutzungsdaten bewertet. Die CNIL betont das gemeinsame europaweite Erfordernis einer Rechtsgrundlage zur Zusammenführung der Einzeldaten. Einschließlich des Zwecks der benutzerangepassten Werbung[11] ist, bezogen auf die einzelnen Dienste, weder ein berechtigtes Interesse, noch ein legitimierendes Vertragsverhältnis und erst recht keine Einwilligung festzustellen. Im Gegenteil stünden einem berechtigten Interesse die schützenswerten Interessen der Nutzer gegenüber der Entstehung eines derart breit angelegten Profils entgegen. Darüber hinaus stünde dem Nutzer keine Einflussmöglichkeit zur Verfügung, mit der er seine Entscheidung gegen eine Zusammenführung seiner einzelnen Nutzungskonten anhand verbindender Daten wie etwa einer übereinstimmenden E-Mail-Adresse durchsetzen könnte. Im Gegenteil werde eine absichtliche Trennung mehrerer Accounts gegen den Willen des Nutzers aufgehoben.

Weiter wird beanstandet, dass Google in seinem Bestreben, Vereinfachungen zu erzielen, deutlich zu wenig und zu vage Informationen zu den Verarbeitungszwecken und Arten personenbezogener Daten gibt. Im Einzelnen werden die fehlende Differenzierung

nach den Diensten bezüglich Zweck und Datenarten, das Fehlen von Löschfristen und die jederzeitige Änderbarkeit der Erklärungen angeführt. Soweit einzelne Angaben sich auf bestimmte Verarbeitungsverfahren bezögen, berücksichtigten die Datenschutzerklärungen den jeweiligen Verarbeitungszweck nicht. Mangels ausreichender Aufklärung könne auch nicht von wirksamen Einwilligungen ausgegangen werden.

Angesichts dessen wird das Einholen wirksamer Einwilligungen in die Zusammenführung und das Einführen verbesserter Kontroll- und Steuerungsmöglichkeiten für den Nutzer gefordert. Bezüglich Google Analytics wird die europaweite Übernahme der für Deutschland vorgesehenen Verfahren gefordert. Für authentifizierte und nicht authentifizierte Nutzer sollen funktionierende, vereinfachte Opt-out-Mechanismen bezüglich der Nutzungsdatenerfassung bereitgestellt werden, die an einem zentralen Ort erreichbar sind.

Bezüglich der Nutzerinformation und Transparenz fordert die Art. 29 Gruppe vollständige Angaben und schlägt ein Vorgehen nach Ebenen vor. Auf der ersten Ebene soll bei den jeweiligen Diensten auf die Datenschutzbelange ausdrücklich hingewiesen werden. In der zweiten Ebene soll eine allgemeine Datenschutzrichtlinie mit Verweisen erstellt werden. Mit der dritten Ebene sollen dienstspezifische Datenschutzerklärungen verfügbar gemacht werden. Gleichzeitig soll eine technische Trennung oder Trennbarkeit der Erfassung von Nutzungsdaten nach einzelnen Diensten sichergestellt werden.

Sanktionen werden mit dem Schreiben nicht angedroht. Allerdings ist dies auch nicht die Aufgabe der Art. 29 Gruppe. Hierfür sind vielmehr die einzelnen nationalen Aufsichtsbehörden der Mitgliedstaaten zuständig.

2.3 Bewertung der Nutzungsbedingungen

Die von Google angebotenen Dienste sind Telemediendienste nach § 1 Abs. 1 Telemediengesetz (TMG). Erfolgt das Dienstangebot aus dem außereuropäischen Raum, wie bei Google Inc. mit Sitz in den USA der Fall, so gilt dennoch das deutsche Telemedienrecht (§ 3 Abs. 5 TMG). Inhaltlich ist die Anwendung des Telemediengesetzes jedoch auf die im Rahmen des Dienstes erhobenen Bestands- und Nutzungsdaten beschränkt. Für Inhaltsdaten gilt das Bundesdatenschutzgesetz,[12] das über § 1 Abs. 5 BDSG ebenfalls auf außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums niedergelassene verantwortliche Stellen Anwendung findet.

Damit hat Google für seine an deutsche Nutzer gerichteten Dienste die Datenschutzvorgaben des Telemediengesetzes (§§ 11 ff TMG) zu erfüllen. Diese wiederum setzen die Datenschutzrichtlinie für elektronische Kommunikation um,[13] so dass der rechtliche Maßstab innerhalb der Europäischen Union weitgehend der gleiche ist.

Die Anforderungen an eine Datenschutzerklärung ergeben sich aus §§ 13 Abs. 1, 15 Abs. 3 Satz 2 TMG. Der Nutzer ist zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten aufzuklären, über eine Verarbeitung der Daten außerhalb des Anwendungsbereichs der europäischen Datenschutzrichtlinie zu informieren und über sein Widerspruchsrecht bezüglich der Erstellung von Nutzungsprofilen zu Werbezwecken hinzuweisen. § 13 Abs. 1 TMG dient der Transparenz vor allem gegenüber dem Nutzer, der in die Lage versetzt werden soll abzuschätzen zu können, wer was über ihn weiß, welche Folgen die Dienstnutzung für ihn haben kann und zu überblicken, ob es sich um eine rechtmäßige Datenverarbeitung handelt.[14]

Welchen Mindestinhalt oder welchen Detaillierungsgrad die Datenschutzerklärung haben muss, um diesen Zweck zu erfüllen, ist nicht weiter festgelegt. Die Erklärung muss jedoch leicht verständlich bleiben.[15] Der Art. 29 Gruppe ist zuzustimmen, dass der Grundansatz, eine Vereinfachung der Datenschutzerklärungen durch Vereinheitlichung und Kürzung herbeizuführen, zu befürworten und in Bezug auf die verwendete Sprache in der zentralen Google-Datenschutzerklärung auch durchaus gelungen ist. Der Gewinn wird jedoch durch die fehlenden Informationen und die fehlende Konsequenz und Übersichtlichkeit bezüglich der parallel fortexistierenden Datenschutzinformationen mehr als aufgehoben. Das wesentliche Ziel des § 13 Abs. 1 TMG, dem Nutzer die Informationen zu geben, die erforderlich sind um informiert über die Preisgabe seiner Daten durch Nutzung des Dienstes oder über die Notwendigkeit eines Widerspruchs zu entscheiden, wird verfehlt. Hierzu trägt bei, dass Google definitive Aussagen über die Datenverwendung vermeidet.

Es liegt auf der Hand, dass auf dieser Grundlage auch keine informierte Einwilligung durch den Nutzer erteilt werden kann. Abgesehen hiervon erfordert eine Einwilligung innerhalb von Nutzungsbedingungen nach § 4a Abs. 1 S. 4 BDSG eine besondere Hervorhebung, auch im Fall elektronischer Erklärungen.[16] Eine konkludente Einwilligung durch Dienstnutzung ist nicht möglich. Google Inc. kann sich bezüglich der Datenerhebungen, die nicht zwingend für den jeweiligen Dienst erforderlich sind oder einem berechtigten Interesse Googles folgen, also nicht auf eine Einwilligung berufen.

Ebenso wird die Zusammenführung der Konten eines Nutzers und der Nutzungsdaten aus verschiedenen Diensten zu Recht kritisiert. Die von Google in der Datenschutzerklärung dargestellte dienstübergreifende Datennutzung verstößt, solange keine wirksame Einwilligung der Nutzer eingeholt wird, gegen § 15 Abs. 3 TMG. Diese Norm erlaubt das Erstellen von Nutzungsprofilen bei Verwendung von Pseudonymen, solange der Betroffene nicht widerspricht. Die Nutzungsprofile dürfen jedoch nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Werden die Daten über das Google-Konto verbunden, findet genau dies statt. Die Konten können zumindest durch die Registrierung den tatsächlichen Namen des Betroffenen mit weiteren Zuordnungsdaten enthalten. Zudem hat der Diensteanbieter nach § 13 Abs. 4 Nr. 4 TMG sicherzustellen, dass die Nutzungsdaten desselben Nutzers bei der Nutzung verschiedener Telemediendienste getrennt verwendet werden können. Eine nachträgliche

Zusammenführung ist rechtswidrig, da keine Erlaubnisnorm für den dienstfremden neuen Verarbeitungszweck vorliegt.

3 Die Hamburgische Lösung zu Google Analytics

Google Analytics ist ein Dienst zur Analyse von Zugriffen auf Internetseiten. Der Website-Anbieter bindet in seine Seite von Google bereitgestellten Script-Code ein (GATC, Google Analytics Tracking Code). Beim Laden der Seite oder Seiten wird ein sog. Beacon, ein praktisch nicht sichtbarer Seiteninhalt, von Registrierungsservern von Google herunter geladen. Außerdem werden bei dem Abruf verschiedene Cookies zur Wiedererkennung des Nutzers gesetzt und weiterer Script-Code geladen. Mit der Anfrage erhält Google Daten über den Nutzer, u.a. welche Seite genau besucht wurde, von wo der Nutzer zu der besuchten Seite geleitet wurde, Daten über den genutzten Browser, seine Einstellungen, das genutzte Betriebssystem und die IP-Adresse, anhand derer der Nutzer einer bestimmten Region zugeordnet werden kann. Durch die gesetzten Cookies kann Google das Nutzungsverhalten auf allen Google Seiten und auf allen Seiten, die Google-Dienste einbinden, verfolgen. Die Datenschutzerklärungen zu Google Analytics versichern jedoch im Gegensatz zur allgemeinen Datenschutzerklärung zu Google Diensten, dass die Nutzungsdaten nicht websiteübergreifend genutzt werden und dass die Datenerhebung durch den Website-Anbieter bestimmt werden kann.[17]

3.1 Inhalt des Kompromisses

Am 26./27. November 2009 veröffentlichte die Arbeitsgruppe der deutschen Datenschutzaufsichtsbehörden, der Düsseldorfer Kreis, einen Beschluss zu den Anforderungen an eine datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten. Gefordert wurden die pseudonyme Erstellung der Profile, eine Widerspruchsmöglichkeit für die Betroffenen, die Löschung der Nutzungsdaten nach erfolgter Analyse oder erklärtem Widerspruch, deutliche Hinweise in der Datenschutzerklärung und entweder die Kürzung der IP-Adresse vor der Auswertung oder das Einholen einer vorherigen Einwilligung.[18] Die Rechtswidrigkeit Google Analytics nach diesen Anforderungen wurde kurz danach offiziell festgestellt.[19]

Auf Basis dieses Beschlusses hat Google Inc. Anpassungen vorgenommen, die von dem Hamburgischen Datenschutzbeauftragten öffentlich im September 2011 als ausreichend anerkannt wurden.[20] Der Einsatz von Google Analytics wird daher als datenschutzkonform akzeptiert, solange die Website-Anbieter, die Google Analytics einsetzen, ebenfalls bestimmte Maßnahmen ergreifen. Bei einer Prüfung von 13.404 Webseiten durch das Bayerische Landesamt für Datenschutz im Mai 2012 wurden diese jedoch nur von etwa drei Prozent der Google Analytics einsetzenden Websites umgesetzt.[21]

Nach der Hamburger Anerkennung müssen folgende Anforderungen erfüllt sein:[22] Die Website-Anbieter müssen einen von Google vorbereiteten und mit dem Hamburgischen Datenschutzbeauftragten abgestimmten Vertrag zur Auftragsdatenverarbeitung abschließen.[23] Der zugehörigen Kontrollpflicht können die Website-Anbieter durch Anforderung von Nachweisen, die Google bereitstellt, nachkommen.

Die Nutzer müssen auf der Google Analytics verwendenden Website in der Datenschutzerklärung über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten aufklären und auf die Widerspruchsmöglichkeit hingewiesen werden. Letzteres soll einen Link auf die Seite https://tools.google.com/dlpage/gaoptout?hl=de umfassen. Google bietet dort für die gebräuchlichsten Browser ein Add-On an, das die Übertragung von Informationen an Google unterbindet.

Die Website-Anbieter haben zudem Google über das Einbinden von weiterem Programmcode in die Website anzuweisen, die IP-Adresse des Nutzers zu kürzen.[24] Die Kürzung wird laut Google in der Regel in Europa durchgeführt und erfolgt vor der Speicherung der Daten. Die diesbezügliche Anleitung richtet sich ausschließlich an Anwender mit Programmiererfahrung. Bezüglich zuvor erhobener Daten wird von dem Website-Anbieter die Löschung verlangt, was nur durch ein Neuanlegen des Trackingauftrags erreicht werden kann.

3.1.1 Datenschutzrechtliche Einschätzung

Aus pragmatischen Gründen mag diese Regelung zu begrüßen sein. Datenschutzrechtlich enthält sie viele Ungereimtheiten und Schwächen. Mit der Kürzung entfällt die Personenbeziehbarkeit der IP-Adresse, so dass anzunehmen wäre, dass mangels Personenbeziehbarkeit das Datenschutzrecht überhaupt nicht mehr eingreift. Bei der Kommunikationsabwicklung mit den Google-Servern wird die IP-Adresse jedoch zunächst vollständig an Google übermittelt, zudem kann die Personenbeziehbarkeit der erhobenen Daten auch auf die Identifizierung mittels der verwendeten Cookies und der verschiedenen personalisierten Google-Dienste gestützt werden. Würde auf letzteres abgestellt, wären die Anforderungen jedoch um weitere Garantien durch Google zu erstrecken. Die den Anforderungen zugrunde liegenden Erwägungen sind jedoch nicht offen gelegt worden. Die Kürzung der IP-Adresse hat zudem der Website-Anbieter gesondert zu veranlassen, worüber von Google nicht sehr offensiv aufgeklärt wird. Aufgrund der vagen Angaben von Google wäre zudem eine Überprüfung des Verfahrens zur IP-Kürzung vor dem Einsatz durch den verantwortlichen Website-Anbieter erforderlich, was diesem jedoch kaum möglich sein wird. Da der Dienst in Europa ohne die Kürzung nicht rechtskonform angeboten werden kann, sollte er von Google innerhalb Europas von vornherein nur unter Einbindung des „_anonymizelp()“-Codes angeboten werden.

Die Erfüllung der Transparenzpflichten nach § 13 Abs. 1 TMG durch die Website-Anbieter setzt voraus, dass für diese hinreichende Klarheit über Art, Umfang und Zweck der Datenverwendung besteht. Diese Klarheit kann der Websitebetreiber nur aus der Datenschutzerklärung und den diversen Erläuterungsseiten von Google erhalten oder er muss sich auf die von Google vorgeschlagene Erklärung verlassen. Nach wie vor sind diese

Angaben jedoch nur mühsam zusammenzustellen, dadurch schwer verständlich und lückenhaft. Weder der Zweck noch der Umfang der Verarbeitung wird genau benannt. Angaben zur Löschung der Daten fehlen ebenfalls. Der Website-Anbieter kann also die geforderte Aufklärung ohne weitere Anpassungen durch Google nicht leisten. Die mit dem Auftragsdatenverarbeitungsvertrag (Abschnitt 8.1) vorgegebene Datenschutzerklärung ist unzureichend, da sie „in Ausnahmefällen" die Übertragung der vollen IP-Adresse in die USA vorsieht. Weiter gelten die Angaben ausdrücklich nur „für den Fall" der IP-Kürzung durch den Website-Anbieter. Genau darüber muss sich der Website-Anbieter jedoch verbindlich erklären. Die Datenschutzerklärung gibt weiter keinerlei Auskunft über die erfassten Daten und spricht als Zweck der Erhebung u.a. von „weiteren mit der Websitenutzung und der Internetnutzung verbundene Dienstleistungen", die Google gegenüber dem Website-Anbieter erbringe.

Die Datenerhebung und –verarbeitung durch Google Analytics soll vollständig durch eine Auftragsdatenverarbeitung erfasst und legitimiert werden. Hierbei ist zu bedenken, dass Google sich die Auswertung zu eigenen Zwecken vorbehält.[25] Eine Auswertung zu eigenen Zwecken durch Google kann jedoch nicht durch eine Auftragsdatenverarbeitung legitimiert werden. Der vorgegebene Vertrag enthält in seinen Anlagen 1 und 2 die durch § 11 Abs. 2 BDSG geforderten Regelungen. Auch hier wird jedoch keine aussagekräftige Beschreibung der Datenverarbeitung nach § 11 Abs. 2 Nr. 2 BDSG gegeben (Abschnitt 2.2.1 ff des Vertrages). Weder die Art der Daten noch die tatsächliche Verarbeitung geht aus der Beschreibung eindeutig hervor. Die Weisungsbefugnisse des Auftraggebers sind so weit unter Vorbehalt gestellt, dass jenseits der möglichen Einstellungen praktisch keine Weisungsbefugnis besteht (Abschnitt 3.2). Eine Regelung zur Mitteilung von Verstößen seitens Google (§ 11 Abs. 2 Nr. 8 BDSG) fehlt völlig, zudem geht der Vertrag davon aus, dass nach der Kürzung der IP-Adressen keine bei Auftragsbeendigung zu löschenden Daten mehr vorhanden sind (Abschnitt 4.2 des Vertrages). Demzufolge wird eine weitere Löschung der erhobenen Daten vermutlich nicht erfolgen. Ob diese jedoch tatsächlich nicht personenbeziehbar sind, ist angesichts der unklaren Aussagen zur Verknüpfung von Daten zwischen den verschiedenen Google-Diensten fraglich. Damit ist die Vertragsvorlage bereits inhaltlich mangelhaft.

Völlig offen bleibt bei den Anforderungen des Hamburgischen Datenschutzbeauftragten, inwieweit überhaupt eine Auftragsdatenverarbeitung durch Google Inc. in Betracht kommt. § 3 Abs. 8 Satz 2 BDSG ist zu entnehmen, dass nur Auftragsdatenverarbeiter innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums keine Dritten im Verhältnis zur verantwortlichen Stelle sind. Dementsprechend würde es sich bei der Einbindung von Google Analytics weiter um eine erlaubnispflichtige Übermittlung personenbeziehbarer Daten an Google handeln. Eine Erlaubnisnorm für diese Übermittlung ist jedoch nicht ersichtlich.[26]

Auch das akzeptierte Widerrufsverfahren per Browser Add-On ist in mehrfacher Hinsicht unbefriedigend. Google behält sich in den schwer verständlichen Nutzungsbedingungen zu seinem Add-On den jederzeitigen Widerruf der zugrunde liegenden Vereinbarung vor.[27] Damit wird die erforderliche Bindungswirkung des Widerrufs fraglich. Ohnehin ist es mit dem anzubietenden Widerspruch kaum vereinbar, dass gleichzeitig Nutzungsbedingungen für dessen Ausübung akzeptiert werden müssen.

Technisch unterliegt das Verfahren ebenfalls einigen Grenzen. So kann das Add-On nur mit bestimmten Browsern verwendet werden. Zudem handelt es sich im Grunde weniger um einen Widerspruch als um ein Verfahren in der Verantwortung oder im Herrschaftsbereich des Nutzers, das die Datenübermittlung verhindert. Änderungen des Browsers, unbemerkte technische Fehler oder unabsichtliche Deaktivierungen des Add-Ons gehen letztlich zu Lasten des Nutzers. Dies entspricht nicht dem Gedanken eines dauerhaft gegenüber der verantwortlichen Stelle erklärten Widerspruchs, für dessen Einhaltung der Erklärungsempfänger verantwortlich ist. Es handelt sich also um eine Kompromisslösung, die durch ein geeigneteres Verfahren zu ersetzen ist, sobald ein solches verfügbar ist.

Eine solche verbesserte technische Lösung könnte in dem Do-Not-Track-Header (DNT) liegen, dessen Standardisierung derzeit gegen erheblichen Lobby-Widerstand im Standardisierungsgremium World Wide Web Consortium (W3C) vorangetrieben wird.[28] Eine Integration der Einstellungsmöglichkeit in den Google Browser Chrome ist kürzlich, wenn auch sehr versteckt, erfolgt.[29] Das DNT-Verfahren erlaubt dienstübergreifende, dauerhafte Browsereinstellungen, durch die Datenschutzinteressen per Defaulteinstellung gewahrt werden könnten. Voraussetzung ist allerdings, dass die Befolgung der durch den Header transportierten Entscheidung des Nutzers für die Dienste-Anbieter flächendekkend Verbindlichkeit erlangt und dass das DNT-Verfahren von den Dienste-Anbietern als Widerspruchverfahren akzeptiert wird. Nach deutschem Recht könnte mit erfolgter Standardisierung davon ausgegangen werden, dass eine Ablehnung des Trackings per DNT-Header wenigstens ein starkes Indiz für ein überwiegendes schutzwürdiges Nutzerinteresse darstellt.

Zuletzt weist auch bereits der Hamburgische Datenschutzbeauftragte daraufhin, dass mit der überfälligen Umsetzung von Art. 2 Nr. 5 der Richtlinie 2009/136/EG[30] („Cookierichtlinie") und des hierdurch geänderten Art. 5 Abs. 3 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) eine Einwilligung des Nutzers vor dem Setzen der Tracking-Cookies von Google Analytics erforderlich wird. Geht man von einer direkten Anwendbarkeit der Richtlinie nach Überschreiten der Umsetzungsfrist aus, wären staatliche Website-Anbieter bereits heute verpflichtet, diese Einwilligung ihrer Nutzer einzuholen. Die derzeitig akzeptierte Lösung ist damit von vornherein zeitlich begrenzt.

Vor allem in Anbetracht des Einwilligungserfordernisses nach dem geänderten Art. 5 Abs. 3 der Richtlinie 2002/58/EG und der nach wie vor unbefriedigenden Transparenz ist die Empfehlung der Art. 29 Gruppe, die für Deutschland vorgesehene Lösung europaweit zu übernehmen, kein empfehlenswerter Schritt.

Website-Anbieter müssen sich beim Einsatz von Google Analytics bewusst sein, dass die öffentliche Erklärung des Hamburgischen Beauftragten für Datenschutz zwar ihr Risiko begrenzt, aber keineswegs dauerhaft Rechtssicherheit schafft. Die übrigen Datenschutzaufsichtsbehörden der Länder sind nicht formal an die Hamburgischen Feststellungen gebunden. Es bestehen weiterhin trotz der Anpassungen durch Google und auch bei Befolgung des Hamburger Kompromissvorschlags schwerwiegende Zweifel an der tatsächlichen Datenschutzkonformität von Google Analytics.[31]

Spätestens die Umsetzung der Richtlinie 2009/136/EG auch in deutsches Recht wird zudem eine Neubetrachtung erzwingen. Weiterer Anpassungsbedarf könnte entstehen, wenn mit der derzeit diskutierten Europäischen Datenschutzgrundverordnung[32] tatsächlich ein Recht auf Vergessen (Art. 17 des Entwurfs), weitere Regelungen zu auf Profiling basierenden Maßnahmen (Art. 20 des Entwurfs) und Vorgaben an datenschutzfreundliche Voreinstellungen (Art. 23 Abs. 3 des Entwurfs) umgesetzt werden sollten.

4 Zusammenfassung

Die Rechtsverstöße bei der Zusammenführung von Nutzerdaten und der Herstellung der erforderlichen Transparenz durch Google nach europäischem oder deutschem Recht sind deutlich. Es ist zudem erkennbar, dass sich bezüglich der Datenschutzbedenken wenigstens ein Teilkonsens weit über Europa hinaus abzeichnet. In den USA hat sich die National Association of Attorneys General mit einem dem Art. 29 Gruppe-Schreiben vergleichbaren Brief noch vor Inkrafttreten der neuen Bedingungen an Google Inc. gewandt.[33] Das Schreiben der Art. 29 Gruppe verweist auf gleichlaufende Untersuchungen im asiatischen Raum.

Es wird an den einzelnen europäischen Datenschutzaufsichtsbehörden liegen, weiter Druck auf Google auszuüben und die angemahnten Änderungen durchzusetzen. Bezüglich der Transparenz führen pragmatische, aber datenschutzrechtlich unbefriedigende Kompromisse nicht weiter. Letztlich liegt es aber auch an den betroffenen Nutzern selbst, das Vorgehen der Aufsichtsbehörden durch ihr Nutzungsverhalten zusätzlich zu legitimieren. Hierzu ist an erster Stelle Aufklärung über die Datenschutzrisiken durch verbundene Dienste, die Rechte und Handlungsmöglichkeiten als Nutzer notwendig. Vorerst ist nicht zu erwarten, dass diese Aufklärung durch die eigentlich verpflichteten Dienste-Anbieter erfolgen wird. Ähnlich dem Verbraucherschutzrecht werden Verbände, Medien, Schulen und weitere staatliche Stellen diese Aufgabe übernehmen müssen. Zusätzlich sollten die gewerblichen Nutzer von Google rechtssichere und rechtskonforme Angebote verlangen, die nicht eine Vielzahl eigener Maßnahmen erfordern, um eine instabile Rechtskonformität zu erreichen.

Solange die Klärung dieser Datenschutzbelange mit Google aussteht, kann Nutzern und Website-Anbietern nur geraten werden, ihre Nutzung von Internet-Diensten auf mehrere Anbieter zu verteilen und statt Google Analytics auf ausgewiesen datenschutzfreundlichere Lösungen zu setzen.

1 Die Erklärung ist abrufbar unter https://www.google.com/intl/de/policies/privacy/archive/20120301/. Reaktionen s. nur unter http://www.heise.de/newsticker/meldung/Google-fuehrt-Dienste-trotz-Datenschutzbedenken-zusammen-1446292.html; s.a. Niclas/von Blumenthal, ITRB 2012, 50; Funke, CR 2012, R26.

2 Abrufbar unter https://www.google.com/intl/de/policies/privacy/

3 S. unter Konto erstellen, https://accounts.google.com/

4 Abrufbar unter https://www.google.com/intl/de/policies/privacy/principles/

5 Informationen werden unter https://www.google.com/intl/de/policies/privacy/tools/ bereitgestellt.

6 Die Einstiegsseite zu den Erklärungen findet sich unter https://www.google.com/goodtoknow/

7 Siehe unter https://www.google.com/goodtoknow/data-on-google/search-logs/

8 Abrufbar unter https://wallet.google.com/files/privacy.html?hl=de

9 PM der CNIL abrufbar unter http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-incomplete-information-and-uncontrolled-combination-of-data-across-ser/

10 Das Schreiben ist abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf

11 Der Anhang des Schreibens identifiziert 8 Zwecke für die Zusammenführung der Nutzungsdaten: die Durchführung von Diensten, bei denen der Nutzer die Zusammenführung wünscht; die Inanspruchnahme von Diensten, die ohne Kenntnis des Nutzers eine Zusammenführung mit sich bringen; Sicherheitsbelange; die Verbesserung und Entwicklung der Angebote; das Angebot des zentralen Kontos; Werbezwecke; Analysezwecke; wissenschaftliche Forschung.

12 Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 12 TMG Rn. 4.

13 Abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF

14 Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 13 Rn. 3; Taeger/Gabel, Kommentar zum BDSG, 1. Aufl. 2010, § 13 Rn. 2.; Heckmann, jurisPK-Internetrecht, 3. Aufl. 2011,Kap. 9, 232.1 f.

15 Härting, CR 2011, 169 (170).

16 Simitis [Simitis], Bundesdatenschutzgesetz, 7. Aufl. 2011, § 4a Rn. 40; .Heckmann, jurisPK-Internetrecht, 3. Aufl. 2011,Kap. 9, 232.

17 Erklärungen zur Datenerhebung und zum Verfahren von Google Analytics finden sich unter https://www.google.com/intl/de/policies/privacy/ads/#toc-analytics und https://www.google.com/intl/de/analytics/privacyoverview.html

18 Beschluss des Düsseldorfer Kreises vom 26./27.11.2009, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf

19 Am 1.7.2010 erklärte die Baden-Württembergische Datenschutzaufsichtsbehörde Google Analytics ausdrücklich für rechtswidrig (https://www.secorvo.de/security-news/secorvo-ssn1008.pdf - Rechtswidrige Webseitenanalyse), bereits vor dem Beschluss des Düsseldorfer Kreises wurde das ULD Schleswig-Holstein aktiv (https://www.datenschutzzentrum.de/tracking/).

20 PM des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, abrufbar unter http://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html.

21 S. PM des Bayrischen Landesamts für Datenschutzaufsicht vom 7.5.2012, abrufbar unter http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2012/pm005.html

22 Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen, abrufbar unter http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_Webseiten-betreiber_in_Hamburg_01.pdf

23 Die Vertragsvorlage ist abrufbar unter http://www.google.de/intl/de/analytics/tos.pdf

24 Google stellt den Code unter https://developers.google.com/analytics/dev-guides/collection/gajs/methods/gaJSApi_gat?hl=de#_gat._anonymizeIp bereit.

25 S. Nutzungsbedingungen zu Google Analytics (Abschnitt 6), abrufbar unter https://www.google.com/analytics/terms/de.html

26 Ähnlich Huth, AnwZert ITR 12/2011, Anm. 2, B I 4.

27 S. unter https://tools.google.com/dlpage/gaoptout/eula.html?hl=de

28 Entwürfe für eine Standardisierung sind unter http://www.w3.org/TR/2012/WD-tracking-compliance-20121002/ und http://www.w3.org/TR/2012/WD-tracking-dnt-20121002/ zu finden. Die Schwierigkeiten, hierbei europäische Datenschutzanforderungen umzusetzen, stellt das ULD dar, abrufbar unter https://www.datenschutzzentrum.de/presse/20121019-selbstregulierung-do-not-track.htm

29 Ankündigung durch Google, abrufbar unter http://chrome.blogspot.de/2012/11/longer-battery-life-and-easier-website.html; s. auch https://www.secorvo.de/security-news/secorvo-ssn1211.pdf

30 RL 2009/136/EG abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:De:PDF

31 Huth, AnwZert ITR 12/2011, Anm. 2.

32 Der Entwurf ist abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF

33 Abrufbar unter http://www.naag.org/assets/files/pdf/signons/20120222.Google%20Privacy%20Policy%20Final.pdf. Das Schreiben äußert Bedenken bezüglich der Änderung der Nutzungsbedingungen ohne Widerspruchsmöglichkeit oder Wahlmöglichkeit der Nutzer, der Datenzusammenführung, der fälligen Neu-Evaluation bzgl. der Nutzung durch staatliche Stellen, der Bindung von Android Nutzern

Kirsten Bock

Do Not Track: Zum Konflikt zwischen Microsoft und der US-Wirtschaft

Die Ankündigung, Microsoft werde seinen Internet Explorer 10 unter Windows 8 mit einer datenschutzfreundlichen Voreinstellung gegen das Tracken auf Webseiten versehen, rief einen Sturm der Entrüstung der US-Industrie hervor. In der Öffentlichkeit wird seit einiger Zeit das stetig dichter werdende Beobachtungsnetz im Internet in Frage gestellt. Die Diskussionen in den USA um einen Do Not Track-Standard zeigen den tiefen Graben zwischen Industrie- und Nutzerinteressen.

Die meisten Menschen möchten sich beim Bummeln und Einkaufen nicht ständig über die Schulter schauen lassen, weder auf der Straße noch im Internet. Viele Menschen glauben dabei, die Datenschutzgesetze würden sie vor einer Beobachtung im Netz schützen. Doch Werbe- und Analyseunternehmen entwickeln immer ausgeklügeltere Verfahren, um Nutzerinnen und Nutzer im Netz zu verfolgen, zu typisieren und online zu identifizieren.

In Europa gibt es seit Dezember 2009 Regeln[1] zum Einsatz von sog. Cookies, wie sie von der Werbeindustrie zur Beobachtung und Identifizierung (Tracking) genutzt werden. Danach ist vor dem Setzen eines solchen Cookies auf dem Rechner einer InternetnutzerIn, deren informierte Einwilligung einzuholen („Opt-In"). In den USA gibt es eine vergleichbare Regelung bislang noch nicht. Dort setzt die zuständige Verbraucherschutzbehörde (Federal Trade Commission, FTC) noch auf eine Selbstregulierung der Internetwerbebranche. Aber die Öffentlichkeit wird ungeduldig. Die zunehmende Personalisierung von Werbeeinblendungen (engl. Online Behavioural Advertising, OBA) macht die NutzerInnen ungehalten. Verbraucherverbände drängen auf ein Bundesgesetz und auf einen Do-Not-Track-Mechanismus, der es ihnen über ihren Browser erlaubt, das Tracking zu kontrollieren. Dies erhöht den politischen Druck. Kann eine einvernehmliche Lösung nicht gefunden werden, so könnte es zu der von der Werbeindustrie gefürchteten gesetzlichen Regelung in den USA kommen.

Sowohl der europäische Gesetzgeber als auch die Regulierer in den USA haben frühzeitig zu erkennen gegeben, dass auch eine browserbasierte Lösung für die Beachtung der NutzerInnenrechte in Betracht komme. Daraufhin bemühte sich das World Wide Web-Konsortium (W3C) um die Definition eines „Do Not Track"-Standards (DNT) als eine technische browserbasierte Lösung. Der Standard soll es NutzerInnen ermöglichen, über ihren Browser Webseitenbetreibern bzw. den darauf werbenden Anzeigenmaklern anzuzeigen, dass sie nicht im Netz verfolgt werden wollen (Do Not Track). In den USA hätte ein solcher Standard weitreichende Folgen. Dort kann die

Verbraucherschutzbehörde FTC bei Anerkennung des DNT-Standards durch ein Unternehmen Verstöße dagegen per Bußgeld ahnen.

Bewegung in die Diskussion um den W3C DNT-Standard kam im Mai diesen Jahres, als Microsoft als erster Browserhersteller einen Vorstoß wagte und ankündigte, den Internet Explorer 10 (IE10) standardmäßig mit der datenschutzfreundlichen Voreinstellung DNT=1 (kein Tracking erwünscht) im Header auszustatten. Was von Datenschützern in Europa einhellig begrüßt wurde, stieß bei der Konkurrenz und der Werbeindustrie auf Ablehnung. Denn sollte diesem Beispiel von anderen Anbietern gefolgt werden, stünde ein erheblicher Einbruch an Werbeeinnahmen in einem Milliarden-Dollarmarkt bevor.

Der Vorstoß von Microsoft führte beim W3C bzw. den dort vertretenen Interessenvertretern der Industrie dazu, dass nun auch öffentlich die Bedeutung des Standards in Frage gestellt wurde und die Meinungsverschiedenheiten über die Interpretation von DNT und dessen Auswirkungen unverblümt offen ausgetragen werden.

Im Kern wird Microsoft vorgeworfen, mit IE10 absichtlich gegen den W3C-Standard verstoßen zu haben. Offenbar hatte man sich im W3C als Grundkonsens zuvor darauf geeinigt, dass der derzeitige Zustand im Internet durch den DNT-Standard erhalten bleiben solle (DNT=unset), so dass es weiterhin jeder NutzerInnen selbst überlassen ist, Maßnahmen gegen die Observation durch die Werbeindustrie zu ergreifen (Opt-out Lösung). Dazu berichtete ZDNet, dass es „politische Gründe“ waren, die „DNT=unset“ Lösung zu wählen, weil die Werbeindustrie das DNT-Signal sonst gar nicht akzeptiert hätte.[2] Dass bei einer solchen Lösung die europäische Rechtslage gänzlich ignoriert würde, scheint die Akteure zunächst einmal nicht gekümmert zu haben.

Als erste Reaktionen auf den „Verstoß“ von Microsoft gegen diesen vermeintlichen Konsens kündigte Yahoo an, dass DNT=1 immer dann ignoriert würde, wenn es von einem IE10 gesendet würde.[3] Ebenso wurde dies von Apache[4], dem immerhin größten Web Server, umgesetzt. Die Begründung klingt gleichermaßen gequält wie absurd: Durch die Voreinstellung sei der DNT-Header nicht aktiv von der NutzerIn gesetzt worden und würde daher den Willen nicht im Netz verfolgt zu werden nicht zum Ausdruck bringen. Daher können man die NutzerInnen des IE10 auch so behandeln, als hätten sie den DNT-Header aktiv auf „Tracking permitted“ (DNT=0) gesetzt und damit im Netz verfolgen. Abgesehen davon, dass nach EU Recht das Verbot mit Erlaubnisvorbehalt das Tracken ohne explizite Einwilligung untersagt, bleibt für die USA unberücksichtigt, dass NutzerInnen den IE10 gerade wegen der datenschutzfreundlichen Voreinstellung nutzen könnten, bzw. sich bewusst für den Erhalt dieser Voreinstellung bei der Installation[5] entscheiden. Zudem zeigen Umfragen, dass die Mehrzahl der NutzerInnen auch in den USA darauf vertraut, dass ihre Browsergewohnheiten zumindest nicht über Webseiten hinaus verfolgt werden.

Der Streit um die Voreinstellung macht auf einen weiteren Verwässerungsversuch des DNT-Standards aufmerksam. Offenbar zielte das Engagement der Werbeindustrie und ihrer Lobbyvertreter in der W3C-Arbeitsgruppe darauf ab, nicht das Sammeln von Informationen über die NutzerInnen einzuschränken, sondern ihnen lediglich keine verhaltensbasierte Werbung auszuliefern. Das heimliche Beobachten und analysieren soll weitergehen wie bisher. Mit einem solchen Standard wäre für die NutzerInnen aber nichts gewonnen. In den USA gaben bei einer Verbraucherstudie[6] die Mehrheit der Befragten an, DNT müsse Werbetreibende davon abhalten, Daten über sie zu sammeln und nicht nur verhaltensbasierte Werbung auszuliefern. Jedoch werden im Netz nicht immer weniger, sondern immer mehr Cookies und Trackingmethoden eingesetzt. Einer Untersuchung des Berkeley Center for Law and Technology[7] zufolge benutzen alle großen Webseiten immer mehr Cookies. Im Oktober 2012 wurden auf den 100 großen Webseiten 6.485 Standard-Cookies gefunden, im Mai 2012 waren es dagegen bloß 5.795. Dabei handelt es sich nicht in erster Linie um sog. First Party Cookies, die von den Webseitenbetreibern selbst gesetzt werden, sondern um Cookies von Werbenetzwerken und anderen Drittanbietern, sog. Third Party Cookies.[8]

Ungeachtet der andauernden Rechtsverletzungen sieht die Werbeindustrie in dem Markt großen Nutzen. Nicht nur im Hinblick auf den eigenen Gewinn: die gewonnen Daten seien das Öl des Internets und von größtem Wert für die Gesellschaft. Als Beiprodukte fördere das Marketing Demokratie, Freiheit und Jobs, so erklärte die Vertreterin der Digital Advertising Alliance (DAA) kürzlich auf der W3C-Sitzung in Amsterdam und forderte gleich, man solle doch die inzwischen sehr gut entwickelten Tracking- und Datensammelpraktiken der Industrie ganz vom DNT ausnehmen: „Marketing should be added to the list of Permitted Uses for Third Parties and Service Providers“ in Section 6.1 of the Tracking Definitions and Compliance Document.“[9] Im Ergebnis bedeutet diese Forderung, die NutzerInnen sollen auch gegen ihren Willen für Marketingzwecke getrackt werden dürfen.

Diese Haltung des Industrieverbandes, zu dem auch Coca Cola, Google und Facebook gehören, repräsentiert allerdings nicht die Haltung und den Wunsch der meisten ihrer Landsleute, wie die Studien aus Berkeley belegen. Allerdings sinken damit die Hoffnungen für einen technischen W3C-Standard.

Kam nun der Vorstoß von Microsoft zu rechten Zeit? Er hat den tatsächlichen Stand der Diskussionen im W3C offengelegt. Von einer Lösung für den europäischen Markt war offenbar nie die Rede. Jacob Kohnstamm, der Vorsitzende des europäischen Datenschutzgremiums (Art. 29 Gruppe) stellte darauf unmissverständlich fest, dass für ein rechtskonformes Do Not Track in Europa

- eine Opt-Out Möglichkeit für die NutzerInnen nicht ausreichend ist
- ein Browser in der Voreinstellung grundsätzlich Tracking Cookies ablehnen muss,
- immer auch die Erhebung der Daten und nicht lediglich nur das Targeting erfasst sein muss
- die Einwilligung der NutzerInnen vor der Erhebung der Daten erfolgen muss
- die Einwilligung nicht durch die Nutzung eines Browsers erfolgen kann, der per Voreinstellung das Tracking erlaubt oder nicht regelt.[10]

Die IE10 Voreinstellung setzt technisch die Grundanforderung des europäischen Gesetzgebers an Browser um. Jedoch setzt eine gesetzeskonforme Nutzung von Cookies weitere Informationen und Einstellungsmöglichkeiten voraus. Für die Zwecke der verhaltensbasierten Werbung erfordert die Voraussetzung der informierten Einwilligung weitergehende Informationen zu den Zwecken der Datenerhebung, der Analysemethoden, der Lebenszeit des Cookies und Widerrufsmöglichkeiten.[11] Eine solche informierte Einwilligung kann durch eine bloße Voreinstellung ohne weitere Informationen nicht erteilt werden. Wie eine solche Lösung aussehen kann, diskutieren seit zwei Jahren Vertreter der EU mit der Industrie und Verbraucherverbänden.

Ohne gesetzlichen Druck wird die Durchsetzung eines DNT-Headers selbst in der Minimalversion in den USA und damit auch für Europa nicht verlässlich sein. Die Interessenvertretung Digital Advertising Alliance (DAA) hat unmissverständlich zum Ausdruck gebracht, dass sie ihn bei ihren Mitgliedern nicht durchsetzten wird.[12] Für die USA ist mit der Besetzung der Spitze der FTC durch eine Demokratin wahrscheinlich, dass das Vorhaben DNT doch nicht scheitert. Senator Jay Rockefeller (DW.Va.) wird weiter auf eine gesetzliche Regelung drängen.[13] Der W3C hat jetzt mit Prof. Swire einen Schlichter in der DNT-Arbeitsgruppe eingesetzt.[14] Offen bleibt aber nach wie vor eine Einigung mit der Europäischen Kommission. Aber auch in Europa lässt die konsequente Durchsetzung des Art. 5 (3) e-Privacy Richtlinie lange auf sich warten. Die Bundesregierung hat die Regelung noch nicht einmal umgesetzt. In Deutschland ist daher die EU-Regelung direkt anzuwenden.[15] Es wäre für alle Beteiligten besser, wenn hier ein fester Zeitpunkt für die Durchsetzung genannt und von den Aufsichtsbehörden auch durchgesetzt würde. Viele Werbenetzwerke sind darauf schon vorbereitet.

1 Art. 5 Abs. 3 der Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG, ePrivacy Richtlinie, auch “Cookie”- Richtlinie genannt)

2 http://www.zdnet.de/88122549/apache-web-server-ignoriert-do-not-track-von-ie10/

3 Yahoo Policy Blog, http://www.ypolicyblog.com/policyblog/2012/10/26/dnt/

4 https://github.com/apache/httpd/commit/a381ff35fa4d50a5f7b9f64300dfd98859dee8d0

5 http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/08/07/do-not-track-in-the-windows-8-set-up-experience.aspx

6 Hoofnagle, Urban, Li, Privacy and Modern Advertising: Most US Internet Users Want „Do Not Track“ to Stop Collection of data About their Online Activities, 8. Oktober 2012

7 Berkeley Law, Web Privacy Census, http://www.law.berkeley.edu/privacycensus.htm

8 Eine schöne Übersicht bietet die New York Times mit ihrem Tracking Barometer, What They Know, The Wall Street Journal, http://blogs.wsj.com/wtk/

9 Centre for Digital Democracy, US Ad Lobby Tries to Hijack Do Not Track, http://www.democraticmedia.org/us-ad-lobby-tries-hijack-do-not-track

10 Jacob Kohnstamm, College Bescherming Persoonsgegevens,

11 Zu den Anforderungen an OBA-Verfahren vgl. https://www.european-privacy-seal.eu/results/Position-Papers

12 http://www.businesswire.com/news/home/20121009005980/en/DAA-Statement-DNT-Browser-Settings

13 http://www.mediapost.com/publications/article/153312/sen-rockefeller-touts-do-not-track-law.html

14 https://www.nytimes.com/2012/11/29/technology/mediator-appointed-in-do-not-track-efforts.html

15 https://www.european-privacy-seal.eu/results/Position-Papers/20110530_e-privacy_Art_5III-en.pdf

Mitgliederverteiler

Für diejenigen unter Ihnen, die Informationen über Presseerklärungen u.ä. auf elektronischem Wege bekommen wollten, gab es bisher nur die Möglichkeit, sich in den öffenltlich zugänglichen Presseverteiler eintragen zu lassen. Das bestehende Angebot haben wir nun ergänzt und bieten unseren Mitgliedern die Möglichkeit, sich in den neu eingerichteten Mitgliederverteiler aufnehmen zu lassen. Wir werden diesen Verteiler ausschließlich nutzen, um über Aktivitäten der DVD zu berichten.

Damit hierüber nur Mitglieder angesprochen werden, bitten wir Sie im Falle Ihres Interesses, entweder der Geschäftsstelle brieflich oder per Fax eine kurze Nachricht zukommen zu lassen oder per E-Mail an schuler@datenschutzverein.de. Bitte nennen Sie Ihren vollständigen Namen und die E-Mail-Adresse, unter der wir Sie anschreiben sollen.

Jens Seipenbusch

Wir speichern nicht

Einleitung

Den Aushang am schwarzen Brett, die Informationsbroschüre vom Amt, den Anzeigenteil der Zeitung – all dies kann man lesen, ohne dass man dabei von jemandem in ein Protokoll eingetragen wird. Nicht immer ist das so in der heutigen digitalen Welt der Informationen. Im Internet hat fast jede Information einen designierten Sender und Empfänger. Ruft man vom heimischen Computer aus die Website eines Informationsanbieters wie z.B. einer Behörde auf, dann wird im Hintergrund automatisch eine Verbindung ausgehandelt, mit der die Information an den eigenen Computer gesendet wird. Die Preisgabe dieser Empfängerinformation, zu der auch die sogenannte IP-Adresse gehört, kann man nicht ohne weiteres verhindern. Oftmals speichern aber die Informationsanbieter im Internet diese Empfängerinformationen über den Zeitraum des Besuchs der Website hinaus. Meistens, ohne dass ein besonderer Grund oder gar eine Berechtigung dafür vorliegt.



Rechtslage

Das Bundesverfassungsgericht hat sich in den letzten Jahren mehrfach mit Fragen rund um den Datenschutz im Telekommunikationsrecht auseinandergesetzt, so heisst es etwa in BVerfG, 1 BvR 1811/99 vom 27.10.2006 : „Auch eine nur kurzfristige Speicherung von Verkehrsdaten berührt das Interesse des Betroffenen an der Wahrung seines Fernmeldegeheimnisses in nicht ganz unerheblichem Ausmaß. Aufgrund der Speicherung kann das Telekommunikationsunternehmen diese Daten zu eigenen Zwecken verwenden. Darüber hinaus besteht die Möglichkeit eines staatlichen Zugriffs, etwa aufgrund des § 100 g StPO. Auch das Risiko eines Missbrauchs der Verkehrsdaten durch das Telekommunikationsunternehmen oder durch Dritte, die sich unbefugt Zugang zu ihnen verschaffen, ist nicht völlig auszuschließen.“ Das gilt auch für Daten, die bei Anbietern von Webseiten gespeichert werden. Mag die Speicherung im Einzelfall auch einfach daraus resultieren, dass Software und Hardware rund um das Anbieten von Websites im Internet oft in ihrer Voreinstellung diese Daten protokollieren, so können sie in Kombination mit anderen digitalen Datenspuren eines Internet-Surfers sehr schnell ein umfassendes persönliches Bild über seine Verhaltensweisen, Vorlieben und Probleme ergeben. Und obwohl staatlichen Behörden wie Polizei und Geheimdiensten eine Identifizierung der Nutzer mithilfe von IP-Adressen unter bestimmten Voraussetzungen erlaubt ist, so will man doch jenseits dessen im allgemeinen die Informations- und Meinungsfreiheit im Internet auch ohne permanente Protokollierung personenbeziehbarer Daten wahrnehmen können.

Projekt

Aus diesem Grund hat der Arbeitskreis Vorratsdatenspeicherung am 01.10.2007 das Projekt „Wir speichern nicht“ gestartet (www.wirspeichernnicht.de). Damit wird auf die oft überflüssige und rechtswidrige Speicherung von IP-Adressen bei den Betreibern von Websites nicht nur hingewiesen, sondern es wird auch ein datenschutzfreundliches Siegel eingeführt, das diejenigen Websites tragen dürfen, die auf eine solche Protokollierung verzichten. Da in diesem Bereich oft große technische und faktische Unsicherheiten und Befürchtungen herrschen, werden auf der Website dieses Projekts auch viele Fragen über die Auswirkungen und Argumente beantwortet, bis hin zu der Möglichkeit, sich untereinander über datenschutzfreundliche Provider oder technische Möglichkeiten auszutauschen.

Fazit

Im Ergebnis braucht es für die meisten Websites meist nur eine kleine Umstellung, um von der pauschalen Protokollierung des Nutzerverhaltens zu einer datenschutzfreundlichen Lösung zu kommen. Für die Funktionen der überwiegenden Zahl von Websites macht dies keinen Unterschied. Auch auf Nutzerstatistiken und ähnliche übliche Besucherauswertungen muss man als Betreiber nicht verzichten. Es lohnt sich für jeden Webseiten-Anbieter, mal auf www.wirspeichernnicht.de vorbeizuschauen, damit auf seiner Webseite der digitale Passant weiterhin unbeschwert flanieren kann.

Frans Jozef Valenta

Nützliche Datenschutz-Tools für den Besuch von Internetseiten

Bis Mitte der neunziger Jahre des letzten Jahrhunderts war Werbung überwiegend auf Printmedien, TV- und Radiowerbung beschränkt. Das Internet hat der Branche eine sehr wesentliche Veränderung gebracht: Nun war zum ersten Mal die Möglichkeit vorhanden, die Werbung auf Effizienz zu überprüfen und Erkenntnisse über das Kundenverhalten zu gewinnen.

Dabei werden die Klickraten oder die besuchten Seiten unmittelbar aufgezeichnet und ausgewertet. Das Ziel der Werbetreibenden ist die Erstellung eines möglichst genauen Bildes potenzieller Kunden im Internet. Das erfordert eine ständige Beobachtung mit speziellen Analyse-Werkzeugen, die mittels Scripting innerhalb der Webseiten meistens unbemerkt vom Besucher ihre Arbeit verrichten. Die Auswertung der dabei anfallenden Daten kann nach einen kontinuierlich protokollierten Zeitraum zu einem sehr detaillierten Persönlichkeitsprofil führen. Das ist zwar der Wunschtraum der Werbefirmen, aber er wird erkauft mit der bewussten Verletzung der Privatsphäre des Webseitenbesuchers.

Glücklicherweise gibt es ein paar kostenlose Hilfsmittel zur Wahrung der Anonymität im Netz. Sie werden nachfolgend kurz vorgestellt.

Eine der Methoden zur statistischen Erfassung von Webseitenbesuchen ist die Platzierung von unauffälligen 1x1 Pixel großen Bildern mit der Farbe des Hintergrunds, deren automatisches Herunterladen registriert wird.

Counterpixel

Dieses Firefox-Add-on sucht nach Zählpixeln auf einer Seite und zeigt das Vorhandensein mit Hinweisen auf die verwendeten Statistik-Services an. Die Programmerweiterung erkennt die Pixel, blockt sie jedoch nicht.



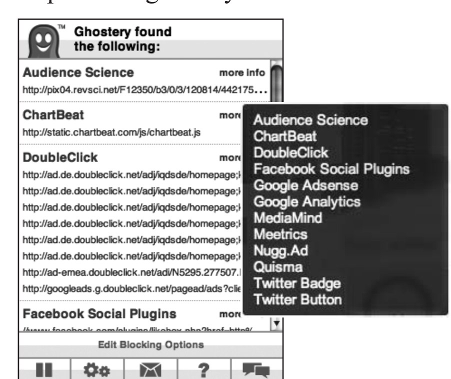
Counterpixel-Webseite:
http://jan.bogutzki.de/counterpixel

Ghostery

Zahlreiche Webseiten, zum Beispiel Google Analytics, Doubleclick oder Facebook Beacon, nutzen Analyse-Tools auf JavaScript-Basis, um Informationen über das Surf-Verhalten auf ihrer Webseite zu erhalten. Ghostery erkennt die beabsichtigte Datensammlung und blokkiert sie bei Bedarf.



Ghostery-Webseite:
http://www.ghostery.com/



Außerdem hält Ghostery zu jedem Script zahlreiche Zusatz-Infos bereit, die Aufschluss über Urheber und Zweck des Trackings geben.

NoScript

Dieses Add-on verfolgt ein anderes Konzept als Ghostery und unterbindet in der Standardeinstellung vorab alle JavaScript-, Java-, Flash- und Silverlight-Elemente einer Seite. Hier ist die Zustimmung des Nutzers erforderlich, um eine Anwendung zuzulassen. Über ein Options-Menü können manuell Webseiten zu einer Liste für ungefährliche Adressen hingezufügt werden. Das ist unter anderem für die einwandfreie Funktionalität beim Online-Banking und die Wiedergabe von YouTube-Videos unumgänglich.



NoScript-Webseite:
http://noscript.net/

Adblock Plus

Das vorrangige Ziel dieser Browser-Erweiterung ist die Entfernung von Werbung. Erreicht wird dies mit Hilfe



einer von den Adblock Plus-Nutzern erstellten und ständig aktualisierten Filter-Datenbank. Das Blockieren der Ladevorgänge funktioniert allerdings nur bei Werbung, dessen HTML-Code nicht Teil der Webseite ist und separat geladen wird.

Request Policy

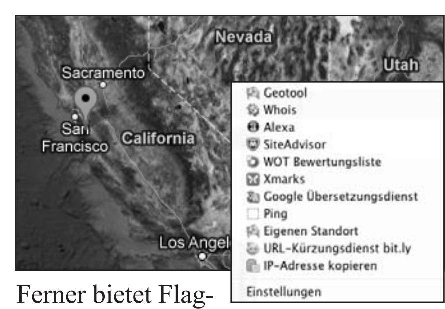
Auch dieses Add-on für Firefox schützt vor domainübergreifenden Webabfragen und ist eine gute Ergänzung zu NoScript.



Request Policy-Webseite: https://www.requestpolicy.com/

Flagfox

Diese Erweiterung zeigt nach Anklicken eines Flaggensymbols den Standort des Servers der aktuellen Webseite als Karte auf Geotool.



Ferner bietet Flagfox eine Reihe weiterer Informationen, z. B. zur Websicherheit, zu WHOIS, DNS mit Seitenbewertung zur Einschätzung der Vertrauenswürdigkeit.



Flagfox-Webseite: http://www.flagfox.net

BugMeNot

Hier handelt es sich um einen Internetdienst, der kostenlos Benutzernamen und Passwörter für anmeldepflichtige Webseiteninhalte anbietet. Dies ist interessant für Benutzer, die sich nicht mit eigenem Namen registrieren wollen. Wer einmal bei Facebook oder Twitter reinschauen möchte, hat hier eine gute Chance, einen Blick hinter den Zaun zu werfen. Von dem Angebot ausgeschlossen sind Pay-per-View-Seiten und Seiten, die Kontodaten der Benutzer enthalten (Banken, eBay, Amazon usw.).



BugMeNot-Webseite: http://www.bugmenot.com/

Robert Malte Ruhland

Haken und Ösen bei der Verwendung von Mitarbeiterfotos durch den Arbeitgeber

Verwendet der Arbeitgeber Fotos seiner Mitarbeiter, hat er eine Reihe von rechtlichen Vorschriften zu beachten. In diesem Artikel soll ein Überblick über die Vielzahl der damit zusammenhängenden rechtlichen Probleme gegeben und Lösungsvorschläge entwickelt werden. Zunächst soll dabei der Schwerpunkt der Betrachtung auf der Herstellung des entsprechenden Bildmaterials liegen, da klar sein dürfte, dass ein rechtswidrig hergestelltes Bild grundsätzlich nicht weiter verwendet werden darf.

I. Herstellung von Bildern der Mitarbeiter

Grundsätzlich ist das Herstellen von Fotos, auf denen Menschen erkennbar dargestellt werden, bis auf wenige Ausnahmen in Deutschland erlaubt. Das bedeutet aber nicht, dass eine Pflicht existiert, sich fotografieren oder filmen zu lassen. Finden Aufnahmen ohne Zustimmung des Fotografierten oder Gefilmten statt, hat dieser jederzeit das sich aus dem allgemeinen Persönlichkeitsrecht ergebende Recht, einer Aufnahme zu widersprechen. Er kann diesem Recht praktisch Ausdruck verleihen, indem er beispielsweise die Fotografie durch Verdecken seines Gesichtes verhindert. Auch heimliche Aufnahmen sind grundsätzlich nicht verboten, solange sie keinen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht darstellen.

Strafrechtlich relevant wird dagegen die Herstellung von Bildaufnahmen erst dann, wenn durch die Aufnahme selbst oder die spätere Verbreitung des gefertigten Bildmaterials die Intimsphäre des Betroffenen beeinträchtigt wird.

1. Fotografierverbot gemäß § 201a StGB

Nach § 201a StGB ist schon das Anfertigen von Bildaufnahmen straf-

bar, wenn diese „unbefugt in einer Wohnung“ oder in einem „gegen Einblicke besonders geschützten Raum“ hergestellt werden und dadurch der „höchstpersönliche Lebensbereich“ der betroffenen Person verletzt wird. Mit dieser als sogenannter Paparazzi-Paragraph im Jahre 2004 durch das 36. Strafrechtsänderungsgesetz geschaffenen Vorschrift wollte der Gesetzgeber der Tatsache Nachdruck verleihen, dass in aller Regel mit unbefugten, d.h. meist heimlich hergestellten Bildaufnahmen, in privater oder intimer Umgebung in der Regel auch ein schwerwiegender Persönlichkeitsrechtseingriff verbunden ist, den es auch strafrechtlich zu ahnden gilt. So findet diese Vorschrift beispielsweise beim Einsatz von sogenannten Spycams in Schlafzimmern, Umkleide- und WC-Räumen Anwendung.

Ob ein herkömmlich eingerichtetes, für die Kollegen ohne weiteres zugängliches Büro ebenfalls zu einem schützenswerten Raum im Sinne dieser Vorschrift gehört, ist bislang noch nicht entschieden und darf angezweifelt werden.

Ein Verbot der Herstellung von Bildaufnahmen kann sich aber auch noch aus einem anderen Gesichtspunkt ergeben.

2. Fotografierverbot als Ausdruck des Hausrechtes

Seit langem ist anerkannt, dass der Eigentümer oder Besitzer eines Grundstückes oder einer Immobilie ein sogenanntes Hausrecht besitzt. Dieses wird in der Regel aus dem § 858 ff., 903, 1004 BGB abgeleitet. Aus diesem Hausrecht ergibt sich nicht nur die Befugnis des Hausrechtsinhabers, im Rahmen der rechtlichen Vorgaben zu entscheiden, wem er Zutritt zu seinen Räumlichkeiten gewährt, sondern auch Bedingungen an diesen Zutritt zu knüpfen. Zu diesen Bedingungen gehört beispielsweise auch ein Fotografier- und Filmverbot.

Ein solches sich aus dem Hausrecht ergebendes Verbot begegnet uns in der Praxis auf Grund einer Vielzahl von rechtlichen Gegebenheiten. So existieren beispielsweise in Theatern, Musicalhallen und Kinos Fotografie- und Filmverbote schon auf Grund des Urheberrechtes. In vielen Firmen und Produktionsstätten bestehen solche Verbote zum Schutz vor Spionage und Geheimnisverrat.

II. Die Verwendung der legal hergestellten Bilder

Ist die Frage der erlaubten Herstellung von Bildaufnahmen geklärt, stellt sich die Frage der zulässigen Verwendung des entsprechenden Materials. Dabei ist für eine rechtliche Beurteilung die Frage erheblich, was mit dem entsprechenden Bildmaterial geschehen soll. Soll das Bildmaterial „verbreitet“ oder „öffentlich zur Schau gestellt“ werden, gilt das Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Fotographie (KunstUrhG) von 1907. Findet dagegen eine Verwendung des Bildmaterials außerhalb des Anwendungsbereiches dieses KunstUrhG statt, ist die Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) zu prüfen.

Es ist daher zunächst die Frage zu klären, wann ein „Verbreiten“ oder „öffentlich zur Schau stellen“ von Bildmaterial zu bejahen ist. Dies ist rechtlich umstritten. Dieser Streit wird noch dadurch genährt, dass sowohl der Begriff des „Verbreitens“ als auch der Begriff des „öffentlich zur Schau stellens“ weder im KunstUrhG noch im BDSG legal, d.h. durch den Gesetzgeber, definiert wurden. Allerdings sind diese Begriffe im ebenfalls in Deutschland geltenden Urheberrechtsgesetzt (UrhG) geregelt. Danach ist unter einer „Verbreitung“ das Recht zu verstehen, „das Original oder Vervielfältigungsstücke der Öffentlichkeit anzubieten oder in Verkehr zu bringen“ (§17 I UrhG). Legt man diese Definition zugrunde, so fällt auf, dass sowohl dem Verbreitungsrecht als auch der öffentlichen Wiedergabe der Begriff der „Öffentlichkeit“ zugrunde liegt. Demnach finden die Regeln des KunstUrhG nur Anwendung, wenn das entsprechende Bildmaterial mit Öffentlichkeitsbezug verwendet wurde. Es stellt sich daher die Frage, wann ein solcher Öffentlichkeitsbezug anzunehmen ist. Dies ist insbesondere bei weltweit agierenden Konzernen relevant. So ist es dort in der Regel üblich, dass auch auf Inhalte, die sich lediglich im firmeninternen Intranet befinden, weltweit von einer großen Anzahl von Personen zugegriffen werden kann. In einen solchen Fall würde sich beispielsweise die Frage stellen, ob sich im Firmen-Intranet befindliches Bildmaterial, welches Mitarbeiter zeigt, nicht bereits veröffentlicht ist. Auch der Begriff der „Öffentlichkeit“ ist weder im KunstUrhG noch im BDSG vom Gesetzgeber legal definiert, so dass sich noch einmal ein Rückgriff auf die Regelung des UrhG empfiehlt. Dort heißt es im § 15 III UrhG bezogen auf das Recht der Wiedergabe durch Bild- oder Tonträger und bezogen auf das Recht der Wiedergabe von Funksendungen sowie auf das Recht von öffentlicher Zugänglichmachung, dass die Wiedergabe dann öffentlich ist, wenn sie „für eine Mehrzahl von Mitgliedern der Öffentlichkeit bestimmt ist“. Dabei gehört jeder zur Öffentlichkeit, „der nicht mit demjenigen, der das Werk verwertet oder mit den anderen Personen, denen das Werk in unkörperlicher Form wahrnehmbar oder zugänglich gemacht wird, durch persönliche Beziehungen verbunden ist“.

Nach der hier vertretenen Ansicht liegt eine solche „persönliche Beziehung“ auch vor, wenn zwischen demjenigen, der für die Verwertung des entsprechenden Bildmaterials verantwortlich ist und demjenigen, dem es bestimmungsgemäß zugänglich gemacht wird, ein vertragliches Verhältnis besteht. Demnach ist der Begriff der „Öffentlichkeit“ und damit auch die Anwendbarkeit des KunstUrhG zu verneinen, wenn der Arbeitgeber entsprechendes Bildmaterial beispielsweise im Intranet ausschließlich seinen Mitarbeitern zugänglich macht. Dass die entsprechenden zugriffsberechtigten Mitarbeiter beispielsweise in einem global operierenden Konzern von jedem Ort der Welt und zu jedem Zeitpunkt auf das entsprechende Material zugreifen können, ändert daran nichts.

Würde man einer anderen Rechtsansicht folgen, hätte man auch die Frage zu beantworten, ab welcher Unternehmensgröße bzw. Mitarbeiterzahl und ab welcher globalen Vernetzung eine Öffentlichkeit anzunehmen ist und bis wann von einer internen Verwendung auszugehen ist. Die Tatsache, dass der Gesetzgeber für die Bejahung des Öffentlichkeitsbegriffes weder die Zahl derjenigen, denen das entsprechende Material zugänglich gemacht wird,

noch die entsprechenden internationalen Verflechtungen regelt, zeigt, das diese Aspekte bei der Frage, wann ein Öffentlichkeitsbezug gegeben ist, außer Acht bleiben müssen.

Folgt man der hier vertretenen Rechtsansicht, so lässt sich relativ einfach zwischen der Anwendbarkeit des KunstUrhG und des BDSG unterscheiden.

So liegt keine öffentliche Verwendung nach der hier vertretenden Rechtsansicht immer dann vor, wenn beispielsweise der Arbeitgeber Abbildungen von Mitarbeitern im Intranet, für betriebsinterne Präsentationen und für Mitarbeiterzeitschriften verwendet, die bestimmungsgemäß nur den Mitarbeitern zugänglich sind.

Ein Öffentlichkeitsbezug ist dagegen zu bejahen, wenn Mitarbeiterfotos im Internet, in frei zugänglichen Werbebroschüren und Werbefilmen und in der Allgemeinheit zugänglichen Zeitschriften verwendet werden.

Im Übrigen wird aber noch zu zeigen sein, dass zumindest bezogen auf die Rechtsfolgen zwischen beiden Gesetzen bei der Frage der Bildnisverwendung keine allzu großen Unterschiede bestehen.

III. Zulässigkeit der Veröffentlichung von Mitarbeiterabbildungen nach dem KunstUrhG

Die Zulässigkeit der Veröffentlichung von Bildnissen auf denen Personen erkennbar dargestellt sind, richtet sich nach dem § 22, 23 KunstUrhG. Für die Anwendbarkeit des KunstUrhG ist Voraussetzung, dass ein Bildnis, welches einen Menschen erkennbar wiedergibt, verbreitet oder öffentlich zur Schau gestellt wurde. Erst wenn alle diese Merkmal kumulativ vorliegen, ist das KunstUrhG anwendbar und es stellt sich weiter die Frage, inwieweit die Verwendung des Fotos unter diesen Umständen zulässig ist. Es ist daher erforderlich, das Vorliegen dieser Voraussetzungen genau zu prüfen.

1. Bildnis

Ein Bildnis im Sinne dieser Vorschriften ist jede individualisierbare Darstellung einer natürlichen Person. Das KunstUrhG ist mithin nur anwendbar, wenn Menschen zumindest auch auf dem entsprechenden Bildnis dargestellt sind. Sind auf dem streitgegenständlichen Bildnis dagegen beispielsweise nur Sachen zu sehen, findet das KunstUrhG keine Anwendung. Vielmehr muss in solchen Fällen eine Beeinträchtigung des allgemeinen Persönlichkeitsrechtes des entsprechenden Besitzers bzw. Eigentümers der abgebildeten Sachen geprüft werden.

Die Form der Darstellung ist für die Anwendbarkeit des KunstUrhG nicht erheblich. Demnach kann ein Bildnis beispielsweise auch aus einem Comic, einer Karikatur oder einer dreidimensionalen Darstellung (z.B. Büste) bestehen.

Ferner werden durch das KunstUrhG nicht nur stehende Bilder (Fotos) sondern auch bewegte Bilder (Filme) umfasst. Auch auf die Qualität der entsprechenden Abbildungen kommt es nicht an. Für die Anwendbarkeit des KunstUrhG ist allein entscheidend, dass die Person, die Ansprüche aus dem Gesetz geltend macht, erkennbar dargestellt worden ist. Dabei werden für die Erkennbarkeit des Abgebildeten keine objektiven Kriterien zugrunde gelegt.

Es ist also nicht erforderlich, dass ein neutraler und objektiver Betrachter die abgebildete Person wiedererkennt. Vielmehr ist es bereits ausreichend, dass die abgebildete Person beispielsweise durch Bekannte wiedererkannt werden kann (Dreier/Schulze, KunstUrhG, 2004, § 22 Rn.: 4). Die Erkennbarkeit muss sich auch nicht allein aus einer Abbildung des Gesichtes ergeben. Vielmehr kann eine Erkennbarkeit sich auch aus den Umständen, sonstigen persönlichen Merkmalen (Tätowierungen, auffälliger Schmuck etc.) ergeben. Aus diesen Gründen kann beispielsweise auch trotz einer Unkenntlichmachung des Gesichtes (z.B. durch einen schwarzen Balken oder einer Verpixelung) eine Erkennbarkeit und somit ein Bildnis zu bejahen sein.

2. Verbreiten und öffentlich zur Schau stellen

Hinsichtlich dieser Merkmale wird auf die bereits oben dargestellte Definition verwiesen. Diese Merkmale sind beispielsweise immer dann erfüllt, wenn Bildnisse von Personen in Büchern, in Zeitschriften, in Kalendern, in Werbeflyern, im Internet auf Homepages, auf Plakaten, in Werbeanzeigen zu finden sind.

3. Die Einwilligung nach den KunstUrhG

Sind die o. g. Voraussetzungen erfüllt, regelt § 22 KunstUrhG, dass grundsätzlich eine solche Verwendung des Bildnisses nur mit der Einwilligung der abgebildeten Person zulässig ist. Mit der Einwilligung ist dabei die vorherige Zustimmung gemeint. Es ist daher nicht ausreichend, den Betroffenen nach Veröffentlichung nach seiner Erlaubnis zu fragen.

Ferner kann nur derjenige eine wirksame Einwilligung erklären, der sich zum Zeitpunkt seiner Erklärung aller entscheidungserheblichen Tatsachen bewusst ist. Dabei ist die Frage, welche Tatsachen für die Einwilligung entscheidungserheblich sind, nicht pauschal, sondern in Abhängigkeit vom Einzelfall zu beurteilen. So wird ein Mitarbeiter eines Feinkostgeschäftes, der sich bereit erklärt hat, auf Plakaten Werbung für Produkte zu machen, grundsätzlich nichts dagegen haben, wenn sein Konterfei zur Bewerbung von Schweineschnitzeln verwendet wird. Handelt es sich bei dem abgebildeten Mitarbeiter aber um einen Menschen moslemischen Glaubens wird die Tatsache, dass dieser Schweinefleisch bewerben soll, sehr wohl entscheidungserheblich sein.

Weiter ist darüber hinaus für die Einwilligung auch die Verwendungsform entscheidungserheblich. So kann ein Arbeitgeber, der die Einwilligung seines Mitarbeiters zur Veröffentlichung von dessen Konterfei in einem Printmedium erhalten hat, nicht zwangsläufig davon ausgehen, dass damit auch die Einwilligung des Mitarbeiters für eine Veröffentlichung im Internet gegeben wurde. Dagegen spricht insbesondere, dass eine Veröffentlichung im Internet schon von ihrem Wesen her, ein wesentlich stärkerer Eingriff in den Rechtskreis des Betroffenen darstellt, als eine Printveröffentlichung. So ist eine Printveröffentlichung in aller Regel auflagenmäßig begrenzt. Auch erfolgt die räumliche Verbreitung eines Printmediums nur selten weltweit. Anders ist es dagegen bei einer Veröffentlichung im Internet. Diese ist räumlich und zeitlich unbegrenzt abrufbar. Selbst nachdem das entsprechende Bildnis auf der

Ursprungsseite entfernt wurde, ist es meistens dennoch in Webarchiven immer noch gespeichert.

Wichtig ist daher, vor einer Bildnisverwendung des Mitarbeiters dezidiert über die Art, das Ausmaß und die Länge der entsprechenden Kampagne zu sprechen.

4. Ausnahmen von dem Einwilligungserfordernis des KunstUrhG

Von dieser Einwilligungserfordernis enthält § 23 drei Ausnahmetatbestände, die in der betrieblichen Praxis eine Rolle spielen. So bedarf es grundsätzlich keiner Einwilligung zur Abbildung, wenn die abgebildete Person lediglich als „Beiwerk" neben einer Landschaft oder „sonstigen Örtlichkeit" erscheint. Wann die abgebildete Person nur als Beiwerk zu einer sonstigen Örtlichkeit anzusehen ist, ist ebenfalls im Einzelfall zu ermitteln. Dabei ist insbesondere die Bildaussage zu berücksichtigen. Geht es beispielsweise um die Geschichte des historischen Firmengebäudes und sind auf dem entsprechenden Foto auch Mitarbeiter zu sehen, dürfte dennoch klar sein, dass hier das Gebäude im Vordergrund der Bildberichterstattung steht und nicht die ebenfalls zu sehenden Personen.

Darüber hinaus darf eine Veröffentlichung von Mitarbeiterfotos ohne die Einwilligung des Abgebildeten erfolgen, wenn es sich bei den abgebildeten Personen um „Personen der Zeitgeschichte" handelt. „Zur Zeitgeschichte" in diesem Sinne zählen dabei alle „Erscheinungen im Leben der Gegenwart, die von der Öffentlichkeit beachtet werden, bei ihr Aufmerksamkeit finden und Gegenstand der Teilnahme oder Wissbegier weiter Kreise sind" (Dreier/Schulze, KunstUrhG, a.a.O. § 23 Rn.: 3 m.w.N.). Die Rechtsprechung unterscheidet weiter zwischen absoluten und relativen Personen der Zeitgeschichte.

Mit relativen Personen der Zeitgeschichte sind dabei insbesondere Personen gemeint, die beispielsweise auf Grund eines konkreten Lebenssachverhaltes, wenn auch zeitlich beschränkt, das Interesse der Öffentlichkeit auf sich ziehen. Dies kann der Vorstandsvorsitzende eines großen DAX-Unternehmens sein, dem der Vorwurf gemacht wird, sein Unternehmen habe Mitarbeiter bespitzelt, genauso wie der Betriebsratsvorsitzende, dem der Vorwurf gemacht wird, sich in seinen Entscheidungen durch sogenannte „Lustreisen" beeinflusst lassen zu haben.

Wird über diese Personen im Rahmen der Berichterstattung über das entsprechende Ereignis mit einer Abbildung berichtet, so ist dies grundsätzlich auch ohne Einwilligung der betroffenen Person auf Grund ihrer Stellung als relative Person der Zeitgeschichte möglich.

Die wohl am meisten im betrieblichen Bereich zur Diskussion führende Ausnahmevorschrift befindet sich aber im § 23 I Nr. 3 KunstUrhG. Danach dürfen „Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben" ohne deren Einwilligung veröffentlicht werden. In der betrieblichen Praxis wird immer wieder die Ansicht vertreten, dass für die Anwendung dieses Ausnahmetatbestandes ausreichend sei, wenn eine Gruppe von mehreren Personen abgebildet werde. Diese Rechtsansicht wird nach Auffassung des Verfassers jedoch nicht der historischen Entstehungsgeschichte der entsprechenden Vorschrift gerecht. So soll mit dieser Vorschrift das Informationsinteresse der Allgemeinheit bzw. die Pressefreiheit gewahrt werden. Dabei geht es bei diesem Ausnahmetatbestand weniger um die abgebildeten Personen als vielmehr um die Dokumentation des durch sie verkörperten Geschehens. Voraussetzung für die Annahme dieses Ausnahmetatbestandes ist es daher, „dass die Versammlung oder der Aufzug als Vorgang gezeigt wird und das nicht nur – einzelne oder mehrere – Individuen abgebildet sind" (Dreier/Schulze a.a.O. § 23 KunstUrhG, Rn.: 19). An dieser Voraussetzung fehlt es regelmäßig, wenn beispielsweise Mitarbeiter dabei gezeigt werden, wenn sie in einer Gruppe zu Mittag essen oder sich in einer Gruppe unterhalten. Nach der hier vertretenen Rechtsaufassung bedarf die Veröffentlichung solcher Fotos daher der Einwilligung der abgebildeten Personen.

5. Form der Einwilligung nach dem KunstUrhG

Anders als das BDSG (s. dazu unten) stellt das KunstUrhG keine besonderen Anforderungen an die Form der Einwilligung. Die Einwilligung nach dem KunstUrhG zur Verbreitung oder öffentlichen zur Schaustellung des Bildnisses ist daher auch mündlich oder sogar konkludent möglich. Im betrieblichen Bereich ist aber immer der Schriftform, schon aus Gründen der besseren Beweisbarkeit, der Vorzug zu geben.

Ferner sind bei der Bildnisverwendung die etwaigen Mitbestimmungsrechte des Betriebsrates zu beachten. So kommt ein Mitbestimmungsrecht beispielsweise dann in Betracht, wenn das veröffentlichte Bildnis Rückschlüsse über die Leistung oder das Verhalten des Mitarbeiters im Betrieb zulässt (beispielsweise eine auf Arbeitsplätze gerichtete Webcam, die ihre Bilder frei zugänglich ins Internet überträgt). Des Weiteren ist eine Mitbestimmungspflicht gegeben, wenn Mitarbeiter verpflichtet werden, ihr Bildnis beispielsweise zu Werbezwecken zur Verfügung zu stellen.

Darüber hinaus sollte beachtet werden, dass das KunstUrhG dem Abgebildeten auch einen postmortalen Schutz zubilligt. So ist beispielweise die Abbildung eines verstorbenen Mitarbeiters im Rahmen eines Nachrufes gemäß § 22 Satz 3 KunstUrhG nur bis zum Ablauf von 10 Jahren nach dem Tod des Abgebildeten nur mit Einwilligung seines ihn überlebenden Ehegattens oder Lebenspartner und aller Kinder zulässig.

6. Dauer der Einwilligung

Insbesondere bei der Verwendung von Mitarbeiterfotos durch den Arbeitgeber ist bislang die Frage rechtlich umstritten, wie mit der Veröffentlichung von zum Veröffentlichungszeitpunkt bereits ausgeschiedenen Mitarbeitern umzugehen ist, wenn die Erstveröffentlichung mit Einwilligung des Betroffenen erfolgte und bei der Erteilung der Einwilligung keine Abreden zum Umgang mit dem Bildnis nach Ausscheiden des Mitarbeiters getroffen wurden. Teilweise wird in der Rechtsprechung die Ansicht vertreten, dass grundsätzlich eine einmal vom Mitarbeiter eingeräumte Einwilligung zur Verwendung seines Bildnisses durch den Arbeitgeber auch über die Beendigung des Beschäftigungsverhältnisses hin-

aus bestehen bleibt (Urteil des LAG Schleswig-Holstein vom 23.06.2010, Az.: 3 Sa 72/10.)

Die Rechtsprechung, die diese Ansicht vertritt, billigt dem betroffenen Mitarbeiter aber ein Widerrufsrecht zu (zur Möglichkeit eines Widerrufes vgl. auch OLG Frankfurt AM, 24.02.11, Az.: 16 U 172/10.) Aus dem KunstUrhG ergibt sich eine solche Regelung jedoch nicht.

Schlüssiger erscheint es dagegen, auf die Umstände des Einzelfalls abzustellen. Hat der bisherige Mitarbeiter beispielsweise seinem Arbeitgeber das Recht eingeräumt, sein Konterfei zu Werbezwecken zu verwenden, so wird man nicht mehr von dieser Einwilligung ausgehen können, wenn der Mitarbeiter mittlerweile ausgeschieden ist und bei einem Mitbewerber seines ehemaligen Arbeitgebers eine neue Beschäftigung gefunden hat. In einer solchen Konstellation wäre mit Hilfe der Auslegung der zum Zeitpunkt der Vereinbarung zugrunde gelegte Wille der Parteien zu ermitteln. Dabei ist kaum denkbar, dass sowohl der Arbeitgeber als auch der Mitarbeiter, wenn sie an den Fall des Ausscheidens gedacht hätten, ein Interesse daran gehabt hätten, dass ein Mitarbeiter eines Konkurrenzunternehmens weiter Werbung für seinen alten Arbeitgeber macht. Zudem könnte ein solches Verhalten möglicherweise auch wettbewerbswidrig sein.

Um solche Probleme jedoch von Anfang an zu vermeiden, empfiehlt es sich, in einer schriftlich festzuhaltenden Vereinbarung mit den abgebildeten Mitarbeitern auch den Umgang mit der Abbildung nach ihrem Ausscheiden zu regeln. Es empfiehlt sich für einen solchen Fall, die Vereinbarung einer sogenannten Aufbrauchfrist, die es dem Arbeitgeber erlaubt, vor dem Ausscheiden des betroffenen Mitarbeiters gefertigte Publikationen, in einem entsprechend zu regelnden Zeitraum noch zu verwenden.

7. Besonderheiten

Vorsicht ist geboten, wenn der Arbeitgeber sich von seinen Mitarbeitern Bildnisrechte „zeitlich, inhaltlich und räumlich unbegrenzt“ übertragen lassen will. Eine solche Vereinbarung erscheint insbesondere dann als nicht haltbar, wenn für eine solche weitreichende Rechteübertragung keinerlei gesonderte, über den normalen Arbeitslohn hinausgehende, Vergütung vereinbart wird.

IV. Zulässigkeit der internen Bildnisverwendung nach dem BDSG

Ist der persönliche und sachliche Anwendungsbereich des BDSG bejaht, stellt sich die Frage, in wieweit eine Verwendung von Mitarbeiterabbildungen außerhalb des Abwendungsbereiches des KunstUrhG zulässig ist. Es dürfte unstreitig sein, dass es sich bei Abbildungen, auf denen Personen erkennbar dargestellt sind, um personenbezogene Daten im Sinne des § 3 I BDSG handelt. Werden solche personenbezogene Daten beispielsweise im Intranet zum Abruf durch die Kollegen bereitgehalten, so liegt zumindest eine „Nutzung“ von personenbezogenen Daten im Sinne des § 3 V BDSG vor. Eine solche Nutzung personenbezogener Daten ist gemäß § 4 BDSG aber nur zulässig, soweit ein Gesetz oder eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Wobei eine solche Einwilligung, anders als die Einwilligung nach dem KunstUrhG, grundsätzlich schriftlich erfolgen muss (§ 4a I Satz 3 BDSG). Ferner ist für eine wirksame Einwilligung nach dem BDSG Voraussetzung, dass die Einwilligung freiwillig erfolgt.

Liegt keine solche Einwilligung des Betroffenen vor, ist nach einem gesetzlichen Erlaubnistatbestand zu suchen, der es dem Arbeitgeber als verantwortlicher Stelle erlaubt, auch ohne Einwilligung des Betroffenen die entsprechende Abbildung zu verwenden. Hier kommt § 32 I Satz 1 BDSG in Betracht. Danach ist der Arbeitgeber, als für die Verarbeitung personenbezogener Beschäftigtendaten verantwortliche Stelle berechtigt, personenbezogene Daten der Mitarbeiter auch ohne deren Einwilligung zu verwenden, wenn dies für die Durchführung des Beschäftigungsverhältnisses „erforderlich“ ist. Welche Bildnisverwendung im Arbeitsverhältnis erforderlich ist, ist dabei im Einzelfall zu ermitteln. Dabei ist der arbeitsvertragliche Pflichtenkreis des Mitarbeiters zu berücksichtigen. Ferner sind betriebliche Notwendigkeiten von einfachen Arbeitserleichterungen abzugrenzen.

Eine erforderliche Bildnisverwendung ist nach der hier vertretenen Rechtsansicht beispielsweise dann anzunehmen, wenn der Arbeitgeber aus Aspekten der Unternehmenssicherheit Mitarbeiterausweise mit Lichtbildern versehen will, um zu kontrollieren, dass nur Berechtigte das entsprechende Gelände betreten.

Eine Erforderlichkeit im Sinne einer betrieblichen Notwendigkeit ist aber abzulehnen, wenn beispielsweise der Arbeitgeber sein im Intranet veröffentlichtes Telefonverzeichnis durch die Bilder seiner Mitarbeiter ergänzen will. Für die Erreichbarkeit der Mitarbeiter ist eine solche Bildnisverwendung nicht zwingend notwendig. Sie stellt lediglich eine Erleichterung dar. In diesem Falle wäre eine Verwendung der Bildnisse der Mitarbeiter nur nach deren vorheriger freiwilliger Einwilligung möglich, wobei das Gesetz in solchen technischen Fällen es auch erlaubt, dass die Einwilligung nicht schriftlich sondern in einer „anderen Form“ erfolgt. Praktischerweise wird in diesen Fällen die schriftliche Einwilligung durch ein Selbstadministrationsrecht der jeweiligen Mitarbeiter ersetzt. Dabei erhält jeder Mitarbeiter die Möglichkeit seine, im internen Telefonverzeichnis abgelegten Daten, selbst zu pflegen und dabei selbst darüber zu entscheiden, ob und wann er welches Bild von sich hochlädt oder löscht.

V. Fazit

Es erscheint bei oberflächlicher Betrachtung als Widerspruch, dass der vermeintlich intensivere Eingriff leichter möglich ist. So ist eine Veröffentlichung von Bildnissen des Mitarbeiters nach dem für diesen Fall anwendbaren KunstUrhG auch bereits auf Grund einer mündlichen Einwilligung möglich. Der vermeintlich schwächere Eingriff, die nur interne Verwendung seiner Bilder, die sich nach dem BDSG richtet, bedarf dagegen grundsätzlich der schriftlichen Einwilligung des abgebildeten Mitarbeiters. Dieser Wertungswiderspruch war jedoch gesetzlich nicht gewollt, sondern ist allein dem Umstand geschuldet, dass sich das BDSG unabhängig von dem seit bereits 1907 in Kraft befindlichen KunstUrhG entwickelt hat und man es schlicht versäumt hat, beide Regelungen aufeinander abzustimmen.

Gemeinsame Pressemitteilung von FoeBuD (jetzt: digitalcourage), Verbraucherzentrale Bundesverband, Campact und der Deutschen Vereinigung für Datenschutz

Bündnis besteht nach Umfrage auf strengem Meldegesetz: Einwilligung nur bei Meldebehörde

Berlin, 21.11.2012. Vor der heutigen Sitzung des Vermittlungsausschusses fordert das Bündnis „Meine Daten sind keine Ware" die Ausschussmitglieder auf, sich für eine echte Einwilligungsregelung beim Verkauf von Meldedaten durch die Meldeämter zu Werbezwecken und Adresshandel einzusetzen. Lediglich von den Adresshändlern selbst vorgelegte Einwilligungen reichten nicht aus. Das belegen auch eine aktuelle Umfrage und ein Hintergrundpapier des Verbraucherzentrale Bundesverbandes (vzbv).

Das Hintergrundpapier zeigt anhand zahlreicher Fallbeispiele, dass die durch unwirksame Einwilligungsklauseln erschlichene Datennutzung in der Praxis weit verbreitet ist [1]. In Zukunft könnten derartige Schein-Einwilligungen auch gegenüber Meldebehörden verwendet werden, um den Abruf von Daten zu legitimieren.

„Die Gefahr von Schein-Einwilligungen lässt sich nur vermeiden, wenn die Einwilligung zur Datenweitergabe schriftlich gegenüber dem Meldeamt erklärt werden muss", sagt Rena Tangens vom Datenschutz- und Bürgerrechtsverein FoeBuD. „Diese Vorgabe muss explizit im Gesetz verankert werden."

„Datenschutz duldet keine Kompromisse. Bürger/innen müssen sich sicher sein können, dass ihre Daten bei staatlichen Stellen wirksam vor systematischem Missbrauch geschützt sind", ergänzt Karin Schuler von der Deutschen Vereinigung für Datenschutz.

Nach einer Online-Umfrage des vzbv-Projektes „Verbraucherrechte in der digitalen Welt" wurden 84 Prozent der Verbraucher/innen nicht zufriedenstellend darüber informiert, dass ihre Daten durch die Meldeämter weiter gegeben werden dürfen [2]. „Transparenz für Verbraucher/innen wird es nur geben, wenn sie ihre Einwilligung gegenüber dem Meldeamt abgeben, statt dem Unternehmen gegenüber", erklärt Projekt-Referentin Michaela Zinke.

Susanne Jacoby vom Kampagnennetzwerk Campact fordert den Vermittlungsausschuss im Namen des Bündnisses daher auf: „Setzen Sie sich für konsequenten Datenschutz ein. Sorgen Sie dafür, dass Daten nur weitergegeben werden dürfen, wenn das Meldeamt selbst eine schriftliche Einwilligung des Betroffenen besitzt!"

Der Vermittlungsausschuss befasst sich heute mit dem Meldegesetz, nachdem der Bundesrat das Gesetz aufgrund gravierender Datenschutzmängel abgelehnt hatte. Das Bündnis „Meine Daten sind keine Ware" wird seine Forderungen ab 16:45 Uhr vor dem Bundesratsgebäude gegenüber den eintreffenden Vertreter/innen des Vermittlungsausschusses vertreten. Den Online-Appell der Kampagne haben inzwischen rund 200.000 Menschen unterzeichnet.

[1] Hintergrundpapier des vzbv zu erschlichenen Einwilligungen http://www.vzbv.de/cps/rde/xbcr/vzbv/datenweitergabe-einwilligungen-hintergrundpapier-vzbv-2012-10.pdf

[2] Umfrage zur Information in Meldeämtern http://www.vzbv.de/cps/rde/xbcr/vzbv/meldegesetz-umfrage-vzbv-2012.pdf

Update: Der VA hat in eine AG delegiert – Entscheidung erst 2013.

ALVARO: EU-Kommission verweigert umfassende Auskunft zu Clean-IT

Brüssel. Zur Antwort der Europäischen Kommission auf seine schriftliche Anfrage zum Forschungsprojekt Clean-IT, erklärt Alexander ALVARO, Vizepräsident des Europäischen Parlaments und Präsidiumsmitglied der FDP:

„Die Kommission bleibt klare Antworten bezüglich Clean-IT schuldig. Nach wie vor ist unklar, wieso dieses Projekt unterstützt wird. Es gibt weiterhin keinen Einblick in den Zeitplan von Clean-IT und mögliche Einsatzgebiete nach Beendigung des Projekts. Die Kommission verweigert eine genaue Auskunft über ihre personelle Beteiligung an dem Projekt und versucht ihre aktive Rolle herunterzuspielen.

Fakt ist jedoch, dass von Anfang an mehrere Generaldirektionen der EU-Kommission tatkräftig in das Projekt involviert waren und nun allein aufgrund der Kritik aus dem EP den Sitzungen fernbleiben werden.

Ähnlich wie beim Forschungsprojekt INDECT werden hier im Namen der Forschung Grundrechte mit Füßen getreten. Transparenz bleibt für die Kommission weiterhin ein Fremdwort. Ich frage mich, warum in Zeiten knapper Kassen und der Gefährdung sinnvoller Projekte wie ERASMUS, mehr als 325.000€ für Orwellsche Überwachungsphantasien ausgegeben werden. Als Liberaler kann ich keinen Grund erkennen, derartige Pläne zu unterstützen."

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Datenschützer beteiligen sich nicht an Stiftung Datenschutz

Die Datenschutzbeauftragten des Bundes und der Länder haben auf Ihrer Konferenz am 07. und 08.11.2012 in Frankfurt/Oder beschlossen, vorerst nicht bei der von der schwarz-gelben Koalition geplanten Stiftung Datenschutz mitzumachen. Dagmar Hartge, die Landesbeauftragte für den Datenschutz in Brandenburg und Vorsitzende der Konferenz der Datenschutzbeauftragten (DSB-K) im Jahr 2012 berichtete, dass man dem Bundesinnenministerium mitteilen werde, die drei eigentlich reservierten Beiratsposten nicht zu besetzen. Hartge benutzte den Begriff des Boykotts nicht. Auch eine Zusammenarbeit mit der Stiftung solle nicht völlig ausgeschlossen werden: „Wir wollen die Tür nicht zuschlagen.“. Kritisiert wurde von den Datenschutzbeauftragten, dass sämtliche Vorschläge aus ihrer Runde für die Stiftung unberücksichtigt geblieben seien. Auf Gesprächsangebote habe das Bundesinnenministerium nicht reagiert.

Ursprünglich sollte die Stiftung Datenschutz einmal so etwas werden wie die Stiftung Warentest: Eine Organisation, die verlässliche Informationen darüber liefert, ob man den Datenschutzregeln eines Web-Dienstes oder anderen Produkts trauen kann, ob die eigenen Daten dort sicher sind. Vier Jahre zuvor hatte die FDP das Projekt auf den Weg gebracht, im Juni 2012 beschloss der Bundestag ein Konzept - da sprachen SPD und Grüne angesichts spärlicher Finanzmittel schon von einem Desaster und bezeichneten die Stiftung als Feigenblatt. Im Entwurf einer Satzung ist vorgesehen, dass der DSB-K, dem Düsseldorfer Kreis als Zusammenschluss der Aufsichtsbehörden und den Bundesbeauftragten jeweils ein Sitz in dem über 30sitzigen Beirat zustehe.

Die Satzung der Stiftung sieht für den Beirat in bestimmten Fällen Verschwiegenheit vor, gleichzeitig sei man als Datenschützer auch für die Aufsicht von Stiftungen zuständig. Deshalb, meinte Hartge, sei eine Mitarbeit in dem Gremium unvereinbar mit der eigenen Unabhängigkeit. SPD und Grüne kündigten an, auch nicht für Beiratsposten zur Verfügung zu stehen. Netzpolitik.org hatte im Juni kritisiert: „Inhaltlich ist von den eigentlichen Aufgaben nicht mehr viel übrig geblieben. Statt effektivem Verbraucherschutz sollen die Interessen der Wirtschaft im Vordergrund stehen. Die Unabhängigkeit ist durch die Angliederung im Innen-Ressort und die Einbindung der Wirtschaft nicht gewährleistet. Nachdem im Februar 2012 die Pläne für die Stiftung bekannt wurden, hatte das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein schon signalisiert: „So wird daraus nichts.“

Der SPD-Datenschutzexperte Gerold Reichenbach erläuterte: „Wir sehen keinen Mehrwert in dieser von der Wirtschaft dominierten Stiftung.“ Der Grünen-Internetexperte Konstantin von Notz bezeichnet die Stiftung in ihrer jetzt geplanten Ausrichtung als eine „Riesenfarce“. Statt Gütesiegel für gute Datenschutzpraxis zu vergeben, solle sie nun „Bildung im Bereich des Datenschutzes“ vorantreiben, etwa Broschüren zum Thema entwickeln. Die finanzielle Ausstattung der geplanten Stiftung sei so dürftig, dass damit nur ein Leiter und zwei Mitarbeiter eingestellt werden könnten. Mit der jetzt geplanten Ausprägung diskreditiere „man den an sich guten Grundgedanken einer Stiftung Datenschutz“. Auch die Vorsitzende der Datenschutzkonferenz Hartge bemängelte die Ausstattung der Stiftung (Stiftung Datenschutz ohne Datenschützer, www.spiegel.de 09.11.2012; Datenschützer verweigern sich der Stiftung Datenschutz, www.zeit.de 09.11.2012; Datenschützer wollen geplante Stiftung vorerst boykottieren, www.sueddeutsche.de 09.11.2012; Datenschutzbeauftragte und Oppositionsparteien boykottieren zahnlosen Tiger, www.netzpolitik.org 09.11.2012, PE 17.02.1012, ULD zur Stiftung Datenschutz: „So wird daraus nichts“).

Bund

2011 mehr große Lauschangriffe

Aus einer Unterrichtung der Bundesregierung auf Basis einer Statistik des Bundesamts für Justiz geht hervor, dass im Jahr 2011 Gerichte in zehn Verfahren eine akustische Wohnraumüberwachung angeordnet haben. Darüber hinaus führte das Bundeskriminalamt (BKA) zur Gefahrenabwehr drei große Lauschangriffe in zwei Verfahren durch. Für 2010 hatte die Justizbehörde zunächst die Genehmigung von vier großen Lauschangriffen in vier Verfahren bekanntgegeben. Die Länder Baden-Württemberg, Hamburg und Niedersachsen meldeten inzwischen noch einschlägige Überwachungsaktivitäten in insgesamt vier weiteren Verfahren nach. 2011 liefen je zwei gerichtliche Vorgänge mit Lauschangriff in Baden-Württemberg, Berlin und Hamburg ab, für Brandenburg und Niedersachsen werden je ein Verfahren ausgewiesen.

Anlass für die Strafverfolgungsmaßnahmen waren schwere Straftaten, darunter in drei Fällen die Bildung krimineller oder terroristischer Vereinigungen sowie ebenfalls dreimal Mord und Totschlag. Als Grund für die Wohnraumüberwachungen zur Gefahrenabwehr

werden länderübergreifende Gefahren des internationalen Terrorismus angegeben. Laut dem Papier verwanzten die Ermittler dabei im vergangenen Jahr insgesamt elf Privatwohnungen und drei „sonstige“ Unterkünfte. Die einzelnen Überwachungen dauerten zwischen einem und 130 Kalendertagen. Relevant für das Ermittlungsverfahren waren die Maßnahmen in acht Fällen, in fünf lieferten sie dafür keine Ergebnisse (Krempl, Ermittler setzten den großen Lauschangriff 2011 häufiger ein, www.heise.de 20.09.2012).

Bund

Strafbarkeits-Initiative gegen Datenhehlerei

Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) will den Ankauf und die Auswertung von Steuer-CDs durch ein Gesetz gegen Datenhehlerei künftig verhindern und unterstützt damit ihren hessischen Kollegen Jörg-Uwe Hahn (FDP), der eine Gesetzesinitiative gegen Datenhehlerei über den Bundesrat auf den Weg bringen will. Ziel der Initiative ist eine Strafbarkeit des Ankaufs und Erwerbs illegal erhobener Daten. Der fertige Gesetzentwurf soll nach den Vorstellungen von Hahn noch in der laufenden Legislaturperiode abgestimmt werden. Mit dem Entwurf soll eine Gesetzeslücke „in der virtuellen Welt“ geschlossen werden. Leutheusser-Schnarrenberger kritisierte zugleich die „Blockade“ der SPD-geführten Länder gegen ein Steuerabkommen mit der Schweiz: „Mit dem Abkommen wollten wir eine legale Grundlage schaffen, um Steuerhinterziehung zu bekämpfen. Ich finde es unverantwortlich, dass SPD und Grüne das Steuerabkommen aus populistischen Gründen scheitern lassen.“

Dagegen hält Schleswig-Holsteins Ministerpräsident Torsten Albig (SPD) solche CD-Käufe für absolut legitim: „Ich bin dafür, alle Steuer-CDs zu kaufen, derer wir habhaft werden können, und sie zu nutzen. Denn das bringt dem Fiskus sehr, sehr viel Geld.“ Für ihn ist die FDP-Initiative „heuchlerisch“, wenn sie behauptet, hier gegen „Hehlerei“ vorzugehen. Die Liberalen erweckten damit den Eindruck, es sei legitim, den Steuerstaat zu beklauen. Die Kronzeugenregelung in Prozessen oder der Unterwanderung organisierter Kriminalität seien Beispiele dafür, dass der Staat immer wieder Kriminelle nutze, um andere Kriminelle zu bekämpfen. Der Preis für Steuerdaten-CDs hängt erheblich von der Aufbereitung der gespeicherten Daten ab. Gemäß Presseberichten hat das Land Nordrhein-Westfalen zuletzt für vier Steuer-CDs weniger gezahlt als zunächst berichtet, weil die schwierige Auswertung der Daten den Preis gedrückt habe. Demnach kostete die CD der Coutts Bank, die von der Düsseldorfer Staatsanwaltschaft bearbeitet wird, nur etwas mehr als eine Million Euro. Ursprünglich waren 3,5 Millionen Euro im Gespräch. Gemäß einem Ermittler hatte es Probleme gegeben, die Klarnamen der SteuersünderInnen herauszufiltern (Ministerin: Ankauf von Steuer-CDs bestrafen, http://www.merkur-online.de 01.09.2012; SZ 16.11.2012).

Bund

Neues umstrittenes Melderegister für Bankberater

Einmütig verurteilen Arbeitgeber und Arbeitnehmer aus dem Versicherungsbereich das neue Melderegister für Bankberater, das seit dem 01.11.2012 in Betrieb ist. Kreditinstitute müssen gemäß dem § 34d Wertpapierhandelsgesetz nun alle ihre 300.000 Mitarbeitenden, die KundInnen zu Geldanlage oder Altersvorsorge beraten, an die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) melden. Damit sollen Falschberatungen bekämpft werden. Die Finanzkrise hatte gezeigt, dass Banken häufig Produkte verkauften, die hohe Provisionen brachten, die KundInnen wenig nützten oder schadeten. Das Melderegister setzt sich aus zwei Bausteinen zusammen. Gemeldet werden zum einen neben den vollständigen Namen, dem Geburtsdatum und genauer Tätigkeitsbeschreibung die jeweilige Qualifikation des Beratenden, beispielsweise Weiterbildungen, Studium und/oder Praxiserfahrung sowie der direkte Vorgesetzte und der Name des Verantwortlichen für Compliance im jeweiligen Institut. Umstritten ist der zweite Teil, wonach die Banken jede Beschwerde einer KundIn an die Bafin weitergeben und den Namen des Mitarbeitenden nennen müssen. Bei Häufung von Beschwerden kann die Aufsicht ein Bußgeld verhängen, in extremen Fällen ein zweijähriges Berufsverbot.

Georg Fahrenschon, Präsident des Sparkassenverbands, kritisiert, es sei nicht klar definiert, was als Kundenbeschwerde gelten soll. Die Folge sei, dass Kreditinstitute jeden Sachverhalt anzeigen müssten, egal ob der berechtigt ist oder nicht, selbst wenn notorische Nörgler sich melden oder auszuräumende Missverständnisse vorlägen: „Mit der Regelung werden Mitarbeiter von Kreditinstituten pauschal an den Pranger gestellt, ohne dass Beschwerden Substanz oder Berechtigung haben müssen. Berater müssen vor Denunziantentum und willkürlicher Unmutsäußerung geschützt werden.“ Das Register kriminalisiere wegen weniger schwarzer Schafe einen ganzen Berufsstand und bedrohe einzelne Mitarbeitende.

Bei den Bankberatern führen die zusätzlichen Kontrollen zu Verunsicherung. Gisbert Straden, Autor des Fachartikels „Sich selbst Vertrauen schenken“ (Bankmagazin 08/2012): „Viele Vertriebsmitarbeiter in Banken sind mit ihrer Arbeit unzufrieden und haben mit Burn-out-Symptomen zu kämpfen. Hinzu kommt, dass die Nichtwürdigung – ob gefühlt oder tatsächlich – der eigenen Arbeitsleistung durch Kunden und auch durch den Arbeitgeber bei vielen Beratern zu Kränkungsempfinden führt, im Extremfall bis zu dem Verlust des Selbstwertgefühls und einer Identitätskrise.“ Die Gewerkschaft Verdi kritisierte über ihr Vorstandsmitglied Beate Mensch fehlenden Datenschutz und den Ansatz des Registers: „Es ist problematisch, dass das Gesetz nicht auf das Unternehmen, sondern auf einzelne Mitarbeiter abzielt. Das muss geändert werden, denn ein einzelner Mitarbeiter hat keinen Einfluss auf die Rahmenbedingungen, in denen er arbeitet.“ Ein handwerklicher Mangel sei es, dass unklar ist, was mit Speicherungen

passiert, wenn ein Arbeitnehmer den Job wechselt: „Verdi wird Berater, die das nicht akzeptieren wollen, bei einer Klage unterstützen."

Die Volksbank Göppingen schuf schon einen Präzedenzfall, indem sie sich weigerte, ihre Bankberater zu melden. Sie will wegen der Verletzung des Rechts auf freie Berufsausübung eine Verfassungsklage gegen das Register erheben. Die Finanzaufsicht Bafin verteidigt das Register, das die Möglichkeiten erweitere, systematischen Falschberatungen von Banken auf die Spur zu kommen. Es gehe erst einmal darum, Beschwerden zu sammeln. Arbeitnehmer und Arbeitgeber würden angehört. Eine Häufung könne darauf hindeuten, dass in einer Bank etwas falsch läuft. Deshalb werde dann das Vertriebsmodell angeschaut. Dorothea Mohn von der Verbraucherzentrale Bundesverband (vzbv): „Die Aufsicht muss wissen, was am Schalter passiert, denn dort wirkt sich übermäßiger Vertriebsdruck am sichtbarsten aus." Das Melderegister werde das Problem der Falschberatung nicht lösen - könne aber abschreckende Wirkung entfalten (Ab November neue Melderegister für Bankberater, http://www.springerprofessional.de, 25.10.2012; Freiberger/ Rexer, Am Pranger, SZ 05..11.2012, 22).

Bund

Werbewirtschaft startet „Deutschen Datenschutzrat Online Werbung"

Die deutsche Internet-Werbewirtschaft hat die Selbstregulierungsinitiative „Deutscher Datenschutzrat Online Werbung" (DDOW) ins Leben gerufen. Der DDOW will auf Webseiten solche Online-Werbung markieren, die ihre Zielgruppe mit Nutzerprofilen genau erfasst (Online Behavioral Advertising, kurz OBA). Den Nutzenden soll die Möglichkeit eingeräumt werden, derartige Werbeformen zu deaktivieren und so die Erfassung seiner Daten zu Werbezwecken besser kontrollieren zu können. Für die Verbraucher manifestiert sich die Initiative durch ein neues Piktogramm, das künftig „direkt an den Werbemitteln" darüber informieren soll, wenn Werbedienstleister nutzungsbasierte Online-Werbung einsetzen. Per Klick auf das Piktogramm wird der VerbraucherIn angezeigt, welche Dienstleister hinter der Datenerhebung und -nutzung stehen. Technisch soll das über den sogenannten Präferenzmanager funktionieren, der die Cookies der Werbetreibenden deaktiviert, entweder alle oder in Auswahl. Cookies sind kleine Dateien, in denen Werbeanzeigen Informationen auf dem Computer des Internetnutzers ablegen können, unter anderem um diesen im Internet wiedererkennen zu können. Der bisher nur als Beta-Version erhältliche Manager kann auf meine cookies.org heruntergeladen werden. Dort will die Werbewirtschaft auch über Cookies im Allgemeinen informieren. Ein alternatives Informationsangebot zu diesem Thema bietet surfer-haben-rechte.de

Manfred Parteina, Hauptgeschäftsführer des Verbandes, erklärte, Selbstkontrolle sei in der Werbewirtschaft schon lange etabliert, um ein eigenverantwortliches Verhalten der Branche zu gewährleisten. Diese werde jetzt mit dem DDOW um eine digitale Komponente erweitert. Ziel sei mehr Transparenz bei nutzerbasierter Online-Werbung. Die Staatssekretärin im Bundeswirtschaftsministerium, Anne Ruth Herkes erklärte: „Effiziente Werbung muss potenzielle Kunden erreichen. Das ist ein nachvollziehbares Ziel." Hierbei könne es aber zum „Konflikt zwischen dem Informationsbedarf der Wirtschaft und dem Recht auf informationelle Selbstbestimmung der Nutzer" kommen. Die Selbstregulierung der Werbewirtschaft sei da ein richtiger Ansatz.

Der Verein Digitale Gesellschaft sieht DDOW kritisch. Vorsitzender Markus Beckedahl meinte, man wolle die Nutzenden für dumm verkaufen und die kommende EU-Datenschutzreform verwässern. Mit Datenschutz habe das wenig zu tun: „Die Onlinewerbewirtschaft speichert das Surfverhalten quer durch das Web und ignoriert dabei auch geltendes europäisches Datenschutzrecht. Das haben sich Bundesregierung wie EU-Kommission nun wirklich lange genug angeschaut. Die nun vorgestellte Selbstregulierungsinitiative ist seit drei Jahren überfällig und äußerst schwach." Der Verein fordert die Gesetzgeber auf Bundes- und Europaebene auf, für klare und eindeutige Rechtsnormen zu sorgen und diese durchzusetzen.

Europaweit ist die Selbstregulierung der Internet-Werbewirtschaft einheitlich geregelt. Das Gegenstück zu DDOW auf EU-Ebene ist EDAA, European Interactive Digital Advertising Alliance. Hinter DDOW steht der Zentralverband der deutschen Werbewirtschaft ZAW und mit ihm seine 40 Mitglieder, unter anderem auch Marktführer Google („Deutscher Datenschutzrat Online-Werbung" ist Datenschutz-Greenwashing, digitalegesellschaft.de 19.11.2012; Online-Werbewirtschaft: Neue Selbstregulierungsinitiative zu Targeting-Werbung, www.heise.de 19.11.2012; Die Branche will sich regulieren, www.taz.de 19.11.2012; Deutschland: Mehr Klarheit bei Online-Werbung, futurezone.at 19.11.2012; Vollmer, Werbewirtschaft startet „Deutschen Datenschutzrat Online Werbung", www.datenschutz.de 23.11.2012).

Kommentar von Marit Hansen, stellvertretende Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD):

„Auf der Webseite von DDOW heißt es: ‚Das Entscheidungsgremium des DDOW besteht aus sechzehn Mitgliedern, die von den Trägerverbänden delegiert und vom Präsidium des ZAW für drei Jahre ernannt werden. Die Zusammensetzung spiegelt die Struktur der digitalen Werbewirtschaft wider.' Datenschutzinteressen und Verbraucherschutzinteressen sind im ‚Deutschen Datenschutzrat' also nicht repräsentiert. Der Begriff ‚Datenschutzrat' suggeriert aber etwas anderes und ist daher irreführend. Stattdessen hätte man ein unabhängiges Gremium mit ausgewiesener Datenschutz-Expertise einsetzen können.

Informierte Einwilligungen der Nutzenden in ein Tracking für nutzungsbasierte Online-Werbung werden mit dem vorgestellten Mechanismus nicht eingeholt; die rechtlichen Anforderungen werden damit weiterhin nicht erfüllt. Die Idee zu mehr Transparenz ist zwar grundsätzlich zu begrüßen. Wer aber das

Angebot genauer analysiert, dem stellen sich viele unbeantwortete Fragen:

In der FAQ wird auf die Frage ‚Enthalten Cookies personenbezogene Daten?‘ die Antwort gegeben: ‚Nein, Cookies von seriösen Anbietern enthalten niemals personenbezogene Daten.‘ Die Darstellungen sind irreführend, da sie nicht erwähnen, dass eine Verkettung von Cookies-Informationen – und hierfür reicht schon eine eindeutige Kennung – sehr schnell zu einem Personenbezug führt.

In der Datenschutzerklärung - und dies betrifft auch die Privacy Policies der eingebundenen Parteien – erfährt man nichts darüber, welche Informationen über die Online-Nutzung erhoben werden. Zu erwarten wären beispielsweise Aussagen zu der IP-Adresse der Nutzerinnen und Nutzer. Auch die Tracker, die im internationalen – und von der Website eingebundenen – Angebot (http://www.youronlinechoices.com/de/) eingebunden werden, werden nicht gesondert erwähnt.

Auf der Webseite http://meine-cookies.org/cookies_verwalten/praeferenzmanager-beta.html kann sich jeder Nutzende über einen Präferenzmanager aus nutzungsbasierten Werbesystemen ausklinken. Nachdem der europäische Gesetzgeber in Art. 5 Abs. 3 der E-Privacy-Richtlinie dies eindeutig regelt hat, ist klar, dass Opt-out nicht ausreicht. Verlangt wird ein Opt-in. In Ermangelung einer zeitgerechten Umsetzung in deutsches Recht ist diese Richtlinie in Deutschland direkt anwendbar. In jedem Fall werden damit die Anforderungen des deutschen Telemedienrechts, wie es laut Bundesministerium des Innern im Einklang mit europäischem Recht auszulegen ist, nicht erfüllt.

In vielen Installationen von Personen, die sich durch Add-ons bereits gegen ein Tracking schützen wollen, funktioniert der Präferenzmanager übrigens nicht. Auch bleiben Flash-Cookies unberücksichtigt.

Der geäußerte Vorwurf der ‚Augenwischerei‘ ist demnach zutreffend. Die User werden in die Irre geführt. Wir haben es hier nicht mit einer validen Selbstregulierungsinitiative des Zentralverbands der Deutschen Werbewirtschaft zu tun. Gefordert ist aber auch der nationale Gesetzgeber. Deutschland hätte Art. 5 Abs. 3 der E-Privacy-Richtlinie längst national umsetzen müssen. Der Anfang 2012 vorgelegte Entwurf für eine Europäische Datenschutz-Grundverordnung enthält die Anforderungen des ‚Privacy by Design‘ und ‚Privacy by Default‘. Diese Prinzipien sollten auch bei der Gestaltung von Internet-Diensten und bei ernsthaften Selbstregulierungsinitiativen berücksichtigt werden. Es genügt nicht, dass besonders interessierte Nutzerinnen und Nutzer durch Klick auf ein Piktogramm Informationen zum Tracking anfordern können. Gemäß ‚Privacy by Default‘ müsste die Standardeinstellung ‚Kein Tracking‘ sein.“

Bund

Nationales Waffenregister startet 2013

Ein nationales Waffenregister soll ab 2013 zentral erfassen, wer welche Schusswaffe besitzt. Ermittler sollen diese Daten elektronisch abrufen können. Bislang waren die Informationen auf 551 lokale Behörden in Deutschland verstreut. Zum Teil werden die Daten dort noch auf Karteikarten gespeichert. Anfragen wurden mitunter erst nach Monaten beantwortet. Bundesinnenminister Hans-Peter Friedrich (CSU) präsentierte damit knapp vier Jahre nach dem Amoklauf von Winnenden ein Konsequenz dieser Tragödie. In Folge des Amoklaufs, bei dem ein 17-Jähriger 2009 insgesamt 15 Menschen erschoss und sich dann selbst das Leben nahm, wurde die zentralisierte Erfassung legaler Schusswaffen und deren Besitzer gefordert.

Bisher sind die Daten über legale Schusswaffen lokal in 551 verschiedenen Behörden erfasst. Die Ämter sollen die Informationen nun an das Bundesverwaltungsamt in Köln melden. Behördenpräsident Christoph Verenkotte erklärte am 19.11.2012, dass mehr als ein Drittel der Daten dort bereits eingegangen waren, der Rest werde bis Ende des Jahres vorliegen. Der Präsident des Bundeskriminalamts (BKA), Jörg Ziercke, wies drauf hin, dass das Register von Sicherheitsbehörden seit langem gefordert werde. Die lokalen Behörden hätten Anfragen mitunter erst nach mehreren Monaten beantwortet. Die einheitliche und elektronisch abrufbare Datensammlung werde Ermittlungen erheblich beschleunigen und erleichtern. Auch die Gewerkschaft der Polizei (GdP) begrüßte das zentralisierte Waffenregister. Beamte könnten nun prüfen, ob an einem Einsatzort eine Waffe im Haus sei. In Deutschland gibt es schätzungsweise rund sechs Millionen registrierte Waffen. Exakte Zahlen zu Waffen im Privatbesitz wird es erst geben, wenn das nationale Waffenregister in Betrieb geht. In einem zweiten Schritt soll in dem Register zudem erfasst werden, welche Stationen eine Waffe vom aktuellen Besitzer über etwaige Vorbesitzer und den Handel bis zum Hersteller oder Importeur durchlaufen hat.

Der Bundestag hatte die Einrichtung des Registers im April 2012 beschlossen. Deutschland erfüllt damit eine EU-Vorgabe, die bis Ende 2014 umgesetzt sein muss. Lorenz Caffier, der Vorsitzende der Innenministerkonferenz der Länder, sagte bei der Vorstellung: „Die örtlich zuständigen Waffenbehörden in Deutschland werden künftig eine Sprache sprechen, egal ob auf der Schwäbischen Alb oder auf der Insel Rügen.“ Dadurch entstehe Rechtssicherheit für Sportschützen, Schützenvereine, Waffensammler, Hersteller und Händler. Die Linke im Bundestag äußerte sich hingegen kritisch: „Innenminister Friedrich ist bekannt für Schnellschüsse, die dann an der Realität oder an handwerklichem Ungeschick scheitern“, sagte der Innenexperte der Fraktion, Frank Tempel. Es sei mehr als fraglich, dass das geplante Nationale Waffenregister Anfang 2013 tatsächlich seine Arbeit aufnehmen kann (Nationales Waffenregister startet im Januar, www.spiegel.de 19.11.2012, Pistolen und Gewehre in einer Datei, www.taz.de 19.11.2012).

Bund

Umstrittenes GETZ nimmt Arbeit auf

Bundesinnenminister Hans-Peter Friedrich eröffnete am 15.11.2012 in Köln ein Gemeinsames Extremismus- und Terrorabwehrzentrum (GETZ).

Bundeskriminalamt und Bundesverfassungsschutz sollen darin die Arbeit der Sicherheitsbehörden im Kampf gegen Terror, Extremismus, Ausländerkriminalität und Spionage koordinieren, um so gefährlicher Personen früher habhaft zu werden.

Das neue Abwehrzentrum ist nicht das erste in dieser Form: Polizeibehörden und Geheimdienste arbeiten bereits in mehreren solchen Einrichtungen zusammen, hinzu kommen Datensammlungen und Beobachtungszentren:

- Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) in Berlin Treptow gibt es schon seit vielen Jahren. Mitarbeiter von 40 Behörden von Bundesverfassungsschutz bis Zollkriminalamt bündeln hier alle Erkenntnisse über islamistischen Terror. Es entstand 2004 als Reaktion auf die Anschläge des 11. September 2001.
- Seit März 2007 besteht zudem die Anti-Terror-Datei (ATD) von Polizei und Nachrichtendiensten. Sie vernetzt terrorismusbezogene Informationen der Polizeibehörden und Nachrichtendienste des Bundes und der Länder. Für jede Behörde sichtbar ist ein Basis-Satz von Daten zu Personen und Einrichtungen. Abfrageberechtigte Behörden können auf besondere Nachfrage aber auch sehen, welche Gefahr von gespeicherten Personen ausgeht. Im Fall eines drohenden Anschlags auch sofort. Die gesetzliche Grundlage für die ATD wird derzeit vom Bundesverfassungsgericht geprüft. Die mündliche Verhandlung hierzu war am 06.11.2012.
- Das im Januar 2007 gegründete Gemeinsame Internetzentrum (GIZ) von Verfassungsschutz und Polizei beobachtet islamistische Terroristen im Internet. Auch hier arbeiten Fachleute des Bundesverfassungsschutzes, des Bundeskriminalamtes, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie der Generalbundesanwaltschaft zusammen. Die Dschihad-Experten sind Techniker und Islamwissenschaftler. Sie verstehen arabisch, sie müssen türkische Websites lesen und Botschaften in Pashtu und Urdu entschlüsseln können.
- Ende 2011, fünf Wochen nach Enttarnung der rechtsextremistischen Terrorgruppe NSU, gründete Friedrich das Gemeinsame Abwehrzentrum Rechtsextremismus (GAR). Es hat Mitarbeiter in Köln, Sitz des Bundesverfassungsschutzes. Weitere Mitarbeiter sind in Meckenheim, wo der Staatsschutz des Bundeskriminalamtes sitzt. Neben Polizei und Geheimdiensten sind auch Europol und der Bundesnachrichtendienst einbezogen. Eine eigene Abteilung wertet rechtsextremistische Websites aus. Friedrich lud auch die Länder ein, sich an dem Zentrum zu beteiligen. Geplant waren zur Gründung bis zu 140 Mitarbeiter.
- In der erst 2012 gebildeten Rechtsextremismusdatei sammeln 36 Sicherheitsbehörden Informationen über gewaltbereite Rechtsextremisten. Jede der Behörden kann sofort auf ausgewählte Angaben zugreifen. Neben dem Bundeskriminalamt gehören der Bundesverfassungsschutz, der Militärische Abschirmdienst und die Bundespolizei sowie die 16 Landeskriminal- und -verfassungsschutzämter dazu.

Wie sehr es an Vernetzung der Sicherheitsbehörden und -dienste fehlt, zeigt die jahrelang erfolglose Suche nach den Mördern des Nationalsozialistischen Untergrunds NSU. Denn im föderal strukturierten Deutschland agieren die etwa 40 Polizei- und Geheimdienstämter von Bund und Ländern weitgehend eigenständig. Bundesinnenminister Friedrich will mit dem GETZ nun die Kooperation verbessern. Dabei stößt es jedoch sowohl wegen des Konzeptes wie auch wegen der Eile auf Widerstand der Länder. Erst Anfang November 2012 stellte der Minister seinen Länderkollegen das schriftliche Konzept des neuen Abwehrzentrums zu, um es zwei Wochen später zu eröffnen. Bei Gründung des Gemeinsamen Abwehrzentrum Rechtsextremismus war der Grund der Eile noch klar. Sämtliche deutschen Sicherheitsverantwortlichen sahen ein, dass Polizei und Geheimdienste auf der Suche nach den NSU-Tätern im großen Stil versagt hatten und die Zusammenarbeit besser werden musste. Es wird seitdem über eine Generalreform der Sicherheitsstruktur diskutiert.

Im August 2012 präsentierte Friedrich ein Reformkonzept für den Verfassungsschutz. Bereits dabei ließen die Länder Friedrich auflaufen, weil sie nicht ohne Grund einen Kompetenzverlust ihrer Landesämter befürchteten. Die erst jüngst gegründeten Abwehr- und Beobachtungsstellen sollten erst einmal Wirkungen entfalten können. Hinzu kommt, dass in der Vielzahl der Zentren stets dieselben Behörden zusammenarbeiten. Mit jeder neuen Koordinierungsstelle wird das vermeintlich von Friedrich angestrebte Ziel der Zentralisierung weiter ad absurdum geführt. Das neue GETZ ist zudem bisher nur wenig mehr als Etikett: Friedrich integriert darin das existente Gemeinsame Abwehrzentrum Rechtsextremismus. Tatsächlich neu ist nur der geplante Bereich Ausländerextremismus, weiterhin eine Abteilung gegen Linksextremismus und eine gegen Spionage.

Insider bezweifeln, ob die Vielfalt der Einrichtungen noch dem Ziel dient, die Arbeit sinnvoll zu bündeln. Aus Sicht seiner Länderkollegen hat der Bundesminister mit dem neuen Abwehrzentrum vollends überzogen. Sie sollen Vertreter von Polizei und Geheimdiensten nach Köln und Meckenheim entsenden und hätten vorher gern mit über Ziel und Aufgabenverteilung entschieden. Vor allem SPD-Minister verweigern die Kooperation. NRW-Ressortchef Ralf Jäger: „Es ist ein Irrtum, wenn Friedrich meint, er könne den Ländern einseitig die Regeln diktieren. Baden-Württembergs Innenminister Reinhold Gall (SPD) kritisierte Friedrichs Vorpreschen und wird vorerst keine Beamten entsenden. „Keine Eile“, hieß es aus Schleswig-Holstein. Das CDU-regierte Hessen sieht Optimierungsbedarf. Sechs Bundesländer haben zunächst Ihre Teilnahme zugesagt. Friedrich verteidigte sich, er habe die Initiative doch bereits im August den Ländern angekündigt.

Trotzig erklärte Friedrich, zunächst gingen dann eben nur die Bundesbehörden in dem neuen Abwehrzentrum an die Arbeit. Die Länder könnten später dazustoßen. Doch ohne die verfehlt das Zentrum seinen Zweck: den Austausch zwischen Bund und Ländern. Zur Innenministerkonferenz Anfang

Dezember hätte Friedrich Gelegenheit gehabt, die Kollegen von seinem Konzept zu überzeugen. Doch die Herbsttagung ist durch das Thema NPD und einen möglichen Verbotsantrag bestimmt. Die Bundestagsabgeordnete Petra Pau von der Fraktion Die Linke kündigte in einem Interview an, ihre Partei wolle eine verfassungsrechtliche Klage gegen das Zentrum prüfen. Sie befürchte eine Verletzung des Trennungsgebots zwischen Polizei und Verfassungsschutz (Streit um Terrorabwehr, SZ 13.11.2012, 6; Steffen, Friedrichs verwinkelter Sicherheitsapparat, www.zeit.de 15.11.2012; Höll, Die kleine Reform, SZ 15.11.2012, 5; Friedrich eröffnet „Neues Super-Abwehrzentrum gegen Terror", www.lto.de 15.11.2012).

Bund/Länder

Weitgehend politische Einigkeit über ein V-Leute-Register

Der Vorstoß von Verfassungsschutz-Präsident Hans-Georg Maaßen für ein zentrales V-Leute-Register findet bei den Bundesländern viel Zustimmung. Als Konsequenz aus den Versäumnissen bei der Fahndung nach der rechtsextremen Terrorzelle NSU schlug Maaßen diesen Informationsaustausch über V-Leute-Einsätze vor, was zugleich als Verzicht auf eine zentrale Führung der V-Leute oder gar „zentralistischen Megabehörde", vor der Nordrhein-Westfalen warnte, ist: „Ein zentrales Wissen ist unabdingbar, um die jeweiligen V-Leute des Bundes und der Landesbehörden für Verfassungsschutz wirksam steuern zu können." Über Einzelheiten für einen besseren Informationsaustausch und eine engere Zusammenarbeit von Verfassungsschützern in Bund und Ländern entscheidet die Innenministerkonferenz Anfang Dezember in Rostock. Bestandteil hiervon soll die zentrale V-Leute-Datei sein.

CDU und SPD unterstützen den Vorschlag Maaßens. Unionsfraktionsvize Günter Krings meinte: „Die Länder müssen ihre V-Leute schleunigst in eine bundesweite Datei einspeisen", sagte er der „Rheinischen Post". Der innenpolitische Sprecher der SPD, Michael Hartmann, ergänzte, der Vorstoß sei überfällig. Der Vorsitzende der Innenministerkonferenz und Mecklenburg-Vorpommerns Ressortchef Lorenz Caffier (CDU) hält ein zentrales Register für denkbar: „Das ist ein Vorschlag, den wir Innenminister sorgfältig erörtern sollten." Baden-Württembergs Innenminister Reinhold Gall (SPD) stimmte zu, meinte aber, dass es wichtiger sei, sich auf Standards und einheitliche Regeln bei der Anwerbung, Führung und Bezahlung von V-Leuten zu einigen. Ein Sprecher des Innenministeriums Thüringen will jedoch weiter die Verantwortung abgeben: „Wir halten weiterhin an der politischen Zielsetzung einer zentralen V-Leute-Führung fest." Aus Niedersachsen wurde erfolgreich gefordert, dass eine solche Datei keine Klarnamen enthalten dürfe. Durch die Speicherung nur der Decknamen ist zweifelhaft, ob über diese Datei herausgefunden werden kann, ob und wer für mehrere Behörden arbeitet. Über die technischen Details soll im Jahr 2013 verhandelt werden. Vereinbart wurden bundesweite Standards für die Zusammenarbeit mit V-Leuten.

Nordrhein-Westfalens Innenminister Ralf Jäger (SPD) warnte vor einer „zentralistischen Mega-Behörde für den Verfassungsschutz". Allerdings müsse der Bund wissen, wo V-Leute in den Ländern eingesetzt werden. Die Zusammenarbeit von Bund und Ländern müsse verbessert werden. Die Führung und die Kontrolle des Einsatzes von V-Leuten sollen künftig nach bundeseinheitlichen Standards erfolgen. Auch Hessen, Schleswig-Holstein, Brandenburg und Bayern unterstützen eine zentrale V-Leute-Datei. Rheinland-Pfalz und Sachsen-Anhalt wollten dagegen den Vorschlag erst einmal prüfen. Die Idee müsse von Bund und Ländern intensiv erörtert werden. Die innenpolitische Sprecherin Ulla Jelpke forderte für die Linke die Abschaltung aller V-Leute: „Nicht die zentrale Erfassung der V-Leute, sondern ihre sofortige Abschaltung muss die Konsequenz aus der Verstrickung von Neonazis und Geheimdiensten sein. Dieser Sumpf muss trockengelegt werden" (Viel Zustimmung für zentrales V-Leute-Register, www.focus.de 05.11.2012; Höll, Die kleine Reform, SZ 15.11.2012, 1, 5).

Baden-Württemberg

Klinik-Sicherungsbänder verschwunden

Eine Sicherungskopie mit mehr als 100.000 Patientendaten aus dem Kreiskrankenhaus Rastatt ist verschwunden. Der Sprecher der Staatsanwaltschaft, Michael Klose, erklärte am 12.10.2012 in Baden-Baden: „Ein gezielter Diebstahl ist eher unwahrscheinlich. Wir können uns keinen Reim darauf machen, wer Interesse an solchen Daten haben könnte." Das Krankenhaus erstellt jeden Tag eine Sicherungskopie, die in einem anderen Gebäude eingeschlossen wird. Die Bänder waren bereits am 19.09.2012 verschwunden. Der EDV-Mitarbeiter hatte die schuhkartongroße Kiste unter den Arm geklemmt und war mehrfach auf seinem Weg zum Safe abgerufen worden, um andere Computer-Probleme im Haus zu lösen. Bei einer Zigarettenpause auf einer Rampe für An- und Ablieferungen stellte er den Karton auf einem Tisch ab und vergaß ihn später. Danach verliert sich die Spur. Klose: „Es gibt keinen Hinweis auf vorsätzliches Handeln". Der Mitarbeiter meldete den Verlust erst am 27.09. Klose: „In der Zwischenzeit hat er auf eigene Faust ermittelt in der Hoffnung, dass irgendein Kollege die Kiste gefunden und aufbewahrt hat". Am 05.10. wurde die Polizei eingeschaltet. „Wir haben dann noch einige Tage mit der Veröffentlichung gewartet, um die Ermittlungen nicht zu gefährden."

Betroffen sind nach Angaben des kaufmännischen Direktors des Klinikverbundes Mittelbaden, Thorsten Reinhardt, Patientendaten aus den vergangenen 16 Jahren: „Wir behandeln pro Jahr etwa 10.000 Patienten stationär und etliche tausend ambulant." Hinzu kämen Hunderte Daten des medizinischen Versorgungszentrums, in dem mehrere ÄrztInnen arbeiten. Zum Klinikverbund, dessen Gesellschafter der Stadtkreis Baden-Baden und der Landkreis Rastatt sind, gehören vier Krankenhäuser in Rastatt, Baden-Baden, Forbach und Bühl. Nachdem der Verlust der Datenträger bekannt wurde, ließ sich die Klinikleitung juristisch beraten und schaltete dann die Polizei und den

Landesbeauftragten für Datenschutz ein. Die PatientInnen wurden am 12.10.2012 mit halbseitigen Anzeigen in den überregionalen Zeitungen „Die Welt“ und „Frankfurter Rundschau“ informiert. Reinhardt: „Das ist bei der großen Zahl der Betroffenen der übliche Weg.“ Nur wenige PatientInnen hätten sich bei der Klinik gemeldet. „Die meisten wollten sich allgemein informieren, einige hatten Angst, dass ihre Krankheitsdaten ihrem Arbeitgeber oder anderen in die Hände fallen könnten“. Reinhardt rief die Betroffenen auf, in den kommenden Wochen verstärkt darauf zu achten, ob an irgendeiner Stelle Informationen über ihren Gesundheitszustand auftauchen. Das Klinikum selbst hat laut Reinhardt seine Sicherheitsmaßnahmen inzwischen verstärkt. „Die Datensicherung und der Transport müssen jetzt immer von zwei Mitarbeitern übernommen werden“ (Kreiskrankenhaus Rastatt - 100.000 Patientendaten verschwunden, www.stuttgarter-zeitung.de 12.10.2012; SZ 13./14.10.2012, 6).

Bayern

BayLDA untersagt Anwaltskanzlei Internetpranger

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat einer bayerischen Rechtsanwaltskanzlei untersagt, die Namen von Personen, die illegal Pornofilme aus dem Internet heruntergeladen haben sollen, auf der Homepage der Kanzlei im Rahmen einer sog. Gegnerliste zu veröffentlichen. Die Kanzlei hatte angekündigt, ab dem 01.09.2012 eine Auswahl der Gegner aus offenen und anhängigen Verfahren, gegen die ihr ein Mandat zur außergerichtlichen oder gerichtlichen Tätigkeit erteilt worden ist, zu veröffentlichen. Die Kanzlei ist im Auftrag der Pornoindustrie mit zahlreichen entsprechenden Abmahnverfahren befasst. Mit der angekündigten Veröffentlichung der Gegnerliste wären Namen von Personen veröffentlicht worden, gegen die sie wegen angeblich illegalen Herunterladens von Filmen beauftragt ist. Die Kanzlei versprach sich von der Veröffentlichung Werbung für sich selbst als auch Druck auf die Verfahrensgegner durch die Prangerwirkung die mit der Information über das illegale Heruntergeladen von Pornofilmen verbunden ist.

Das BayLDA teilte der Kanzlei mit, dass die geplante Veröffentlichung datenschutzrechtlich unzulässig sei und forderte sie auf, diese zu unterlassen. Nach Verstreichen der gesetzten Frist verbot das BayLDA der Kanzlei mit einer für sofort vollziehbar erklärten Anordnung vom 29.08.2012, die Namen oder sonstige personenbezogene Daten von Privatpersonen, gegen die sie wegen Urheberrechtsverletzung, insbesondere wegen Herunterladens von Pornofilmen, beauftragt ist, im Rahmen einer sog. Gegnerliste auf ihrer Homepage oder sonst im Internet zu veröffentlichen. Diese Veröffentlichung von Angaben über Privatpersonen im Internet verletze die betroffenen Personen in ihrem Persönlichkeitsrecht und sei rechtswidrig. Eine gesetzliche Grundlage für die Veröffentlichung bestehe nicht. Die Betroffenen hätten ein überwiegendes schutzwürdiges Interesse, nicht auf solchen Gegnerlisten genannt zu werden. Zweifellos dürfte die Kanzlei für sich werben, aber nicht so.

Selbst wenn davon auszugehen sei, dass die Rechtsanwaltskanzlei die Namen der Gegner nur in den Fällen erhalten habe, in denen durch gerichtliche Entscheidung Internetprovider verpflichtet worden seien, die Namen ihrer Vertragspartner für die IP-Adressen herauszugeben, die beim illegalen Herunterladen von Daten aus dem Internet benutzt worden seien, sei die Aufnahme dieser Namen auf Gegnerlisten im Internet unzulässig. Dabei mache es keinen Unterschied, ob es sich um Namen von Personen, die zu einem früheren oder späteren Zeitpunkt zivil- oder strafrechtlich wegen illegalen Herunterladens verurteilt wurden oder vielleicht noch werden oder ob es sich um Personen handle, die nachweislich keinen illegalen Download vorgenommen haben bzw. denen eine derartige Handlung nicht nachgewiesen werden könne. Die mit der Aufnahme in zu veröffentlichende Gegnerlisten erfolgende Prangerwirkung führe zu einer unverhältnismäßigen Beeinträchtigung des allgemeinen Persönlichkeitsrechts der Betroffenen. Dies gelte insbesondere in den hier zur Diskussion stehenden Fällen des Vorwurfs des illegalen Downloads von Pornofilmen. Die Kanzlei erklärte, bis zum Abschluss eines gerichtlichen Verfahrens keine Gegnerlisten zu veröffentlichen (BayLDA PM vom 03.09.2012).

Bayern

Daten von Allianz-Detektiv abhandengekommen

Polizeiliche und staatsanwaltliche Ermittlungsakten, Asylanträge, Zeugenaussagen und andere Unterlagen wurden der Presse zugespielt, die der europaweit größte Versicherungskonzern Allianz mit Sitz in München einem Privatdetektiv für Ermittlungszwecke zur Verfügung gestellt hatte. Zuweilen beauftragen Versicherungsunternehmen Detektive, um zu ermitteln, ob es für einen Schadenfall die Versicherungssumme zahlen muss. Ein Beispiel für die öffentlich gewordenen Daten ist der Fall eines Schwelbrandes im Dezember 2007, bei dem in einer Erotik-Videothek 20.000 DVDs beschädigt wurden. Der Firmeninhaber ließ diese DVDs von einer Firma reinigen und neu verpakken und zahlte dafür genau 243.942,56 Euro, um sie dann für 37.000 Euro an eben jene Firma zu verkaufen - ein merkwürdiges Geschäft, zumal die Firma einem Bekannten des Unternehmers gehört. Die Allianz zahlte 190.000 Euro für den Brandschaden aus - nicht aber, ohne allen Verdachtsmomenten nachzugehen und alle Akten abzuheften und vorher einen Detektiv eingeschaltet zu haben. Die Allianz bestätigt, dass diese und andere Unterlagen aus ihren Akten stammen. Ein Privatdetektiv habe den Fall bewerten sollen - obwohl der Sache nicht nachgegangen wurde, habe er wohl die Daten widerrechtlich nicht vernichtet und jetzt an die Presse weitergegeben.

Es ist bei Versicherungsunternehmen üblich, mit Privatdetektiven zusammenzuarbeiten, wenn es den Verdacht auf einen Betrug gibt. In diesem Fall fordert das Unternehmen die Ermittlungsakten bei Polizei oder Staatsanwaltschaft an und stellt sie dem Privatermittler zur Verfügung - zumeist in elektronischer Form. In den Unterlagen fan-

den sich auch Informationen, bei denen der Zusammenhang mit einem Versicherungsfall nur schwer zu erkennen ist, etwa der Asylantrag eines Mannes, der inklusive der Daten der Ehefrau und der minderjährigen Kinder aufgenommen wurden. Ein Sprecher der Allianz erklärte, es handele sich hier um einen Einzelfall. Der private Ermittler hätte die weitergegebenen Unterlagen vernichten müssen. Dies sei widerrechtlich nicht geschehen, da die Verträge vorsähen, dass alle Beteiligten sich an die Datenschutzrichtlinien halten müssen. Externe Ermittler hätten keinen Zugriff auf die Datenverarbeitung der Allianz. Das Vertragsverhältnis zu dem Privatdetektiv sei im konkreten Fall bereits im Jahr 2011 auf Betreiben des Chief Compliance Officer der Allianz beendet worden. Der Detektiv habe nicht die transparentesten Abläufe gehabt und sei deshalb nicht weiter beschäftigt worden. Die Allianz bearbeite jährlich in allen Versicherungssparten insgesamt 3,3 Mio. Schadenfälle. Bei der Sachversicherung gebe es in 3-4% Verdachtsmomente. Bei 1% setze die Versicherung externe Ermittler ein. Detektive würden bei 0.03% der Schadenmeldungen tätig. Zum Zeit des Bekanntwerdens des Falls gab der Allianz-Konzern an, mit 13 Detekteien zusammenzuarbeiten. Es bestünden Überlegungen, nur noch zwei bundesweit tätige Ermittlungsfirmen zu beauftragen: „Wir werden strukturierte Qualitätsaudits einführen“. Außerdem überprüfe das Unternehmen, in den Vereinbarungen mit Detekteien Vertragsstrafen bei Verstößen vorzusehen (Fromme/Gröger/Boesler, Detektive sollen schuld sein, Datenpanne schreckt Allianz auf, www.ftd.de 20.08.2012; Kwasniewski, Datenpanne zeigt Sammelwut der Allianz, www. spiegel.de 21.08.2012; Kuntz, Allianz der Detektive, SZ 22.08.2012, 24).

Berlin

Millionenfach polizeiliche Handydatenabfragen

Die Berliner Polizei greift bei ihren Ermittlungen auch nach Kritik (vgl. DANA 1/2012, 23) weiter zu der umstrittenen Funkzellenabfrage. Der Berliner Senat teilte auf einer Sitzung des Innenausschusses am 27.08.2012 mit, dass von 2009 bis Juli 2012 in 1408 Fällen Daten von den Mobilfunkprovidern gesammelt worden sind Anfang des Jahres waren erstmals Zahlen bekannt geworden, seitdem sind 128 Verfahren mit insgesamt 200 Funkzellenabfragen hinzugekommen. 302 Verfahren im Zeitraum 2009 bis April 2012 wurden genauer aufgeschlüsselt. Dabei sind mehr als 6,6 Millionen Datensätze im Rahmen von 302 Abfragen ausgewertet worden. Bei der nicht-individualisierten Funkzellenabfrage wird ausgewertet, welches Handy zu welchem Zeitpunkt in einem bestimmten Gebiet war. 5.383 Mal wurde demnach der Anschlussinhaber ermittelt, woraus sich schließlich 116 „neue Ermittlungsinhalte“ ergaben.

Der Chef der Berliner Piratenfraktion Christopher Lauer kritisierte die Datenabfrage als unverhältnismäßig. Mehrere tausend Unschuldige seien so in den Fokus von Ermittlungen geraten, „nur weil sie sich zu einem bestimmten Zeitpunkt in der Nähe einer Straftat aufgehalten haben.“ Die Berliner Piraten fordern einen restriktiveren Einsatz sowie dass Betroffene nach der Abfrage informiert werden müssen. Die Polizei setzte die massenhafte Abfrage unter anderem ein, um Autobrandstiftern auf die Spur zu kommen. Der Senat hat 302 Verfahren im Zeitraum von 2009 bis April 2012 genauer aufgeschlüsselt. Dabei handelt es sich in 33 Verfahren um Ermittlungen in Zusammenhang mit Brandstiftung. In 215 Verfahren ging es um bestimmte Bandendelikte, in 15 um Mord oder Totschlag, in 31 um Raub oder Erpressung, in 4 um Vergewaltigung und in 3 um Betäubungsmitteldelikte

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) Alexander Dix führte eine Stichprobenprüfung von Funkzellenabfragen der Strafverfolgungsbehörden zwischen 2009 und 2011 durch und stellte dabei gravierende Mängel fest. So sei häufig nicht (ausreichend) geprüft worden, ob eine Funkzellenabfrage im Einzelfall verhältnismäßig war, also der Erforschung einer Straftat von erheblicher Bedeutung diente, und die Ermittlungen auf andere Weise aussichtslos oder wesentlich erschwert waren. Zudem seien die gesetzlich vorgeschriebenen Benachrichtigungs-, Kennzeichnungs- und Löschpflichten nicht beachtet worden. Den Strafverfolgungsbehörden empfahl Dix, künftig durch Dienstanweisungen für mangelfreie Verfahren zu sorgen und die Rechte der Betroffenen in den zurückliegenden Verfahren – soweit erforderlich und noch nicht erfolgt – unverzüglich umzusetzen. Auch solle sich das Land Berlin für Änderungen der bundesgesetzlichen Regelungen einsetzen. Die Vorgaben der Strafprozessordnung zur Durchführung von Funkzellenabfragen und zum Umgang mit den dabei erhobenen personenbezogenen Daten seien zu konkretisieren. Darüber hinaus sollten Berichtspflichten der Strafverfolgungsbehörden gegenüber den Parlamenten und den zuständigen Landesdatenschutzbeauftragten festgelegt werden. (Berlin fragt millionenfach Handydaten ab, www.spiegel.de 27.08.2012; BlnBDI PE v. 04.09.2012).

Hessen

Körperscanner im Frankfurter Flughafen

Auf dem Flughafen Frankfurt wird erstmals drei Körperscanner im Normalbetrieb eingesetzt. Bei einem zehn Monate dauernden Test am Flughafen Hamburg bis Ende Juli 2011 hatten sich die Geräte noch als zu unzuverlässig erwiesen. Nach Überarbeitung der Scanner setzt die Bundespolizei ab sofort in Frankfurt die „nächste Generation“ ein, allerdings nur für Passagiere, die in die USA reisen, und nur, wenn diese es wollen. Der Sprecher der Bundespolizei Christian Altenhofen erläuterte bei der Vorstellung am 23.11.2012, dass gemäß EU-Bestimmungen Passagiere nicht dazu gezwungen werden dürfen, durch einen Körperscanner zu laufen: „Die Alternative ist dann eine manuelle Kontrolle.“

Aus Rücksicht auf das Schamgefühl der Betroffenen zeigen die Körperscanner des US-Unternehmens L3 Communications – im Gegensatz zum sog. Nacktscanner – nur eine Art Strichmännchen. Falls es beim Scan Auffälligkeiten gibt, sind die entsprechenden Körperstellen markiert, so dass

die Beamten gezielt nachkontrollieren können. Realistische Körperbilder werden weder erstellt noch gespeichert. „Die Geräte arbeiten mit aktiver Millimeterwellentechnologie, welche keine gesundheitlichen Auswirkungen hat.“ Scanner mit Röntgenstrahlen werden in Deutschland nicht eingesetzt.

Beim Probebetrieb am Hamburger Flughafen hatten mehr als 800.000 Passagiere die Scanner genutzt. In knapp der Hälfte der Fälle war es zu Fehlalarmen gekommen. Bei weiteren 15% habe es sich, so das Bundesinnenministerium, um echten Alarm gehandelt; bei 5% blieb die Ursache für die Meldung unklar. Nur in 31% der Gesamtfälle gab das Gerät grünes Licht, weil es nichts Verdächtiges bei dem Passagier gefunden hatte. Alarm hatten bereits Falten in der Kleidung, Manschettenknöpfe oder Schweißflecken unter den Achseln ausgelöst. Passagiere, die bei dieser elektronischen Prüfung aufgefallen waren, mussten danach aufwendig per Hand abermals kontrolliert werden. Die Passagierabfertigung wurde verzögert statt beschleunigt und somit ein wichtiges Ziel der Scanner verfehlt. Die für die Passagierkontrolle verantwortliche Bundespolizei betonte, dass es sich bei dem nunmehr erfolgenden Einsatz „grundsätzlich nicht um einen erneuten Testbetrieb“ handelt. Die Leistungsfähigkeit sei verbessert. Die Körperscanner werden aufgrund erhöhter Sicherheitsanforderungen zunächst bei Reisen in die USA eingesetzt. Auslöser für den Einsatz der Scanner war der vereitelte Sprengstoffanschlag eines Nigerianers auf ein US-Passagierflugzeug Ende 2009. Der Mann hatte den Sprengstoff in seiner Unterhose versteckt und wollte die Maschine mit dem Gemisch aus Pulver und Flüssigkeit abstürzen lassen. Die üblichen Sicherheitsschleusen mit Metalldetektoren finden solche Stoffe nicht, ebenso wenig Keramikmesser.

Der Bundesdatenschutzbeauftragte Peter Schaar kündigte an, den Betrieb der Körperscanner in Frankfurt „kritisch zu begleiten“ und auf die Einhaltung der vom Bundesinnenministerium gegebenen Zusagen hinsichtlich des Datenschutzes zu achten. Es müsse sichergestellt sein, dass die Geräte weder individuelle Körperkonturen noch Geschlechtsmerkmale oder künstliche Körperteile darstellten. Auch dürften die Daten nicht gespeichert werden (Umstrittene Kontrollen: Frankfurter Flughafen setzt Körperscanner ein, www.spiegel.de 23.11.2012; Frankfurter Flughafen setzt Körperscanner ein, www.sueddeutsche.de 23.11.2012).

NRW

Polizei überprüfte jahrelang Besucher der eigenen Webseite

Die Polizei in Nordrhein-Westfalen (NRW) ließ jahrelang Besucher von eigenen Websites überwachen. Diese liefen darauf Gefahr, polizeilich verdächtigt zu werden. Gemäß einer Antwort des nordrhein-westfälischen Innenministeriums auf eine Kleine Anfrage der Piratenpartei (LT-Drs. 16/1128) bedienten sich die Polizeibehörden des Landes zwischen 2001 und 2010 mindestens 19 Mal der durch das Bundeskriminalamt (BKA) im Auftrag vorgenommenen „Homepageüberwachung“. Die Maßnahmen wurden teilweise mehrere Wochen oder Monate, in einem Fall sogar ganze sechs Jahre lang heimlich durchgeführt. Dabei wurden sämtliche Zugriffe auf die Seiten gespeichert und ausgewertet. Bei vermeintlich auffälligen Zugriffen wurden die Anschlussinhaber hinter den jeweiligen IP-Adressen ermittelt in der Annahme, dass insbesondere die gesuchte Person an Informationen über die Fahndung nach ihr interessiert ist und deshalb die sie betreffende Webseite besonders häufig aufruft.

Die Erfolgsquote blieb gering. Gemäß NRW-Innenminister Ralf Jäger liegen nur in einem einzigen Fall „nachvollziehbare Erkenntnisse vor, wonach Hinweise aus dieser Maßnahme in Kombination mit anderen Spuren zur Identifizierung und Festnahme von zwei Tätern führten“. Der Bochumer Landtagsabgeordnete Dirk Schatz von der Piratenpartei, im vorparlamentarischen Leben Polizeikommissar, hält die Maßnahme für „völlig rechtswidrig“, weil „eine Masse von Leuten, die völlig unschuldig sind, in Verdacht geraten“.

Die Bundesministerien der Justiz und des Inneren entwickelten hinsichtlich der Methode rechtliche Bedenken. In einem Schreiben vom Februar 2009 an die Landesjustizverwaltungen wies das Justizministerium darauf hin, dass der Einsatz dieses Instruments „zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung“ führe. Beeinträchtigt sei zudem das Grundrecht, „sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten“. Das Bundesinnenministerium hat deshalb „das Unterlassen von Maßnahmen zur Homepageüberwachung veranlasst“. Nach eigenen Angaben hat das BKA seitdem keine Homepageüberwachung mehr durchgeführt.

Im April 2009 wies auch das nordrhein-westfälische Innenministerium die Polizeibehörden des Landes an, diese Maßnahme nicht mehr von sich aus anzuwenden. Verzichten wollten die Ermittler jedoch auf das Instrument offenkundig trotzdem nicht. In einem Mordfall führte das Polizeipräsidium Mönchengladbach noch im Jahr 2010 eine Homepageüberwachung durch, abgesichert durch eine Anordnung des Amtsgerichts Krefeld, was Piratenpolitiker Schatz als eine „ganz klare Fehlentscheidung des Gerichts“ ansieht.

Unklar bleibt, ob es „nur“ insgesamt 19 Homepageüberwachungen in Nordrhein-Westfalen gegeben hat, weil die Auskunft des NRW-Landesinnenministeriums in einem Punkt von einer Antwort des Bundesinnenministeriums auf eine schriftliche Frage des Aachener Linkspartei-Bundestagsabgeordneten Andrej Hunko abweicht, worin Mitte September 2012 mitgeteilt wird, dass das Bundeskriminalamt zwischen 2001 und 2008 in 38 Fällen Besucher seiner Webseite bka.de überwacht hat (BT-Drs. 17/10696, S. 8f.). In weiteren 130 Fällen habe das BKA Länderdienststellen bei Homepageüberwachungen unterstützt. Darüber hinaus habe die Bundespolizei 2006 der Polizei in Nordrhein-Westfalen und der zuständigen Staatsanwaltschaft „eine Webseite mit einer Öffentlichkeitsfahndung innerhalb der Bundespolizeiinternetpräsenz zur Verfügung gestellt“. Hier erfolgte die Überwachung „jedoch nicht durch die Bundespolizei, sondern lag in der Zuständigkeit des Polizeipräsidiums

Essen“. Diese Homepageüberwachung taucht in der Antwort an den Landtag in NRW nicht auf. Der Pirat Schatz will wegen dieses Widerspruchs, „der aufgeklärt werden muss“, nachhaken (Beucker, Den Besuchern nachspioniert, www.taz.de 18.10.2012).

Sachsen

Staatskanzlei zieht Überwachungsplane zurück

Die Landesregierung in Sachsen hat erst nach heftigen Protesten Pläne aufgegeben, Online-Netzwerke systematisch zu überwachen. Die Staatskanzlei plante, Software für 390.000 Euro Software zur systematischen Überwachung sozialer Netzwerke im Internet zu beschaffen. Mit diesem „Social Monitoring“ wollte sie sich „abstrakte Meinungsbilder ohne Personenbezug“ beschaffen und auf Trends reagieren. Staatskanzleichef Johannes Beermann (CDU) teilte dann August 2012 mit, er habe noch einmal mit seinen Mitarbeitern „über den Sinn diskutiert“ und entschieden, dass das Projekt nicht weiterverfolgt werde. Man könne mit Suchprogrammen preiswerter nach Stichworten und frei verfügbaren Daten suchen. Am 15.06.2012 wurde die Ausschreibung einer Software veröffentlicht, die von der Verwaltung vorbereitet worden war. Der Staatskanzleichef will sich erst im August damit befasst haben.

Die Grünen-Landtagsfraktion war auf die Ausschreibung aufmerksam geworden und stellte eine Kleine Anfrage. Sächsische Medien berichteten vom „Sachsen-Trojaner“ und von „Schnüffel-Software“. Die vom Innenminister Markus Ulbig unterzeichnete Antwort auf die Anfrage versucht, die Kritik zurückzuweisen. Nach Ansicht des grünen Landtagsabgeordneten Johannes Lichdi hat das Vorhaben aber nichts mit Öffentlichkeitsarbeit zu tun, sondern zeuge von einem „anmaßenden Staatsverständnis“. Die Ausschreibung schließe Personenbezüge bei der Analyse nicht aus. Einen solchen Ausschluss forderte der sächsische Datenschutzbeauftragte Andreas Schurig. Dessen Vorgänger Thomas Giesen nannte in einem Gastbeitrag der Sächsischen Zeitung die beabsichtigte Anschaffung „ein Werkzeug zur rechtswidrigen und schuldhaften Verletzung der Privatsphäre“ und verwies auf die dahinter stehende Einstellung der Staatsregierung. Weil diese „Denke“ sich nicht verändert habe, erklärten die Grünen, werde man am Thema bleiben (Bartsch, Sachsen Stoppt Schnüffelplan, www.taz.de 10.08.2012).

Schleswig-Holstein

Piratenabgeordneter schnitt heimlich Ausschusssitzung mit

Der Abgeordnete der Piratenfraktion im Landtag von Schleswig-Holstein Uli König hat eingeräumt, eine öffentliche Ausschusssitzung ohne Wissen der Anwesenden „für persönliche Zwecke“ mit dem Mikro seines Laptops aufgezeichnet zu haben. Auf der Website der Fraktion wurde dies am 28.08.2012 bekannt gegeben. Der „private Tonmitschnitt“ sei „nicht kopiert oder verbreitet und bereits am nächsten Tag von mir gelöscht und überschrieben“ worden, so der Pirat: „Erst hinterher wurde mir mein Fehler bewusst. Das wird nicht wieder vorkommen“. Die Sitzung hatte am 08.08.2012 stattgefunden. Dadurch, dass er seine AusschusskollegInnen nicht über die Aufzeichnung informierte, habe König, so die Fraktion, die Persönlichkeitsrechte der Anwesenden verletzt, sich in „Widerspruch zum Recht auf informationelle Selbstbestimmung“ und zu den Grundwerten der Piratenpartei gesetzt. Fraktionschef Patrick Breyer erläuterte: „Uli König hat seinen Fehler eingesehen, korrigiert und steht dazu. Für uns Piraten hat der sensible Umgang mit persönlichen Daten einen sehr hohen Stellenwert und dabei wird es auch bleiben.“

CDU-Fraktionschef Johannes Callsen meinte: „Da fehlen einem fast die Worte“. SPD-Fraktionschef Ralf Stegner reagierte mit Ironie: „Wie die Piraten es mit Transparenz halten, wissen wir inzwischen.“ Für FDP-Fraktionschef Wolfgang Kubicki ist „diese Truppe eher mit einer Kinderkrabbelgruppe vergleichbar denn mit erwachsenen Politiker“. Er hatte den Piraten eine Woche zuvor vorgeworfen, sie missbrauchten die Vertraulichkeit parlamentarischer Gremien. Die Piraten hatten zuvor Interna des Ältestenrats öffentlich gemacht und waren dafür von anderen Fraktionen gescholten worden. Ihren Angaben zufolge seien sie zu Runden der Parlamentarischen Geschäftsführer daraufhin nicht mehr eingeladen worden. Die Piraten betonen, dass nur solche Informationen diskutiert wurden, die keine persönlichen oder geheimen Daten betreffen. Die sechs Abgeordneten sitzen seit der Wahl im Mai 2012 im Kieler Parlament, auch in drei weiteren Landtagen sind Piratenfraktionen vertreten (Piraten-Abgeordneter schnitt heimlich Sitzung mit www.spiegel.de 29.08.2012, PM Piratenfraktion im Schleswig-Holsteinischen Landtag 28.08.2012; Kieler Nachrichten 30.08.2012, 13)

Datenschutznachrichten aus dem Ausland

Weltweit

Staatliche Stellen intervenieren verstärkt bei Google

Gemäß einem von dem Unternehmen am 13.11.2012 veröffentlichten Transparenzbericht hat Google in der ersten Hälfte des Jahres 2012 den deutschen Behörden Daten zu insgesamt 2007 Nutzerkonten weitergegeben. Gerichte und Behörden haben außerdem in 247 Fällen das Löschen von Inhalten verfügt. Staatliche Stellen und Strafverfolger verlangen von Google weltweit immer häufiger die Übergabe von Nutzerdaten. Im ersten Halbjahr 2012 stieg die Zahl der entsprechenden Verfügungen global auf annähernd 21.000 Fälle. Im ersten Halbjahr 2011 lag die Zahl der Fälle noch bei knapp 16.000 Fällen. An der Spitze der Länderliste stehen mit 7969 Verfügungen die USA - in dieser Zahl sind auch internationale Anfragen enthalten. Es folgen Indien (2319), Brasilien (1566) und Frankreich (1546). Deutschland liegt vor Großbritannien mit 1533 Fällen auf Platz 5. In 39% der Fälle hat Google gemäß seinem Bericht die Anfragen aus Deutschland beantwortet, betroffen davon waren insgesamt 2007 Nutzerkonten. Von Juli bis Dezember 2011 hatte der Konzern aus Deutschland 1426 Anfragen erhalten und diese in 45% der Fälle beantwortet. Betroffen waren davon 2027 Nutzerkonten.

William Echikson, der Leiter des Transparenz-Büros von Google in Brüssel, nannte diese Zahlen besorgniserregend: „Wir reden hier von demokratischen Staaten.“ Auffällig sei, dass einige dieser Staaten sich auf der einen Seite für den Datenschutz gegenüber Unternehmen einsetzten, selbst aber immer häufiger Einblick in die Daten ihrer Bürger haben wollten. Ein prominenter Fall des Datenzugriffs ist in diesen Zahlen wohl noch gar nicht enthalten: Mindestens ein E-Mail-Konto der Autorin Paula Broadwell bei Google wurde offenbar vom FBI ausgeforscht. Die Ermittler hatten sich dazu einen richterlichen Beschluss besorgt. Dabei kam heraus, dass die Biografin von David Petraeus mit genau diesem eine Affäre hatte. Letztlich trat der CIA-Chef deswegen zurück.

Einen Sonderfall vermerkt Google für Deutschland: Nach der Klage von Bettina Wulff entfernte das Unternehmen acht Ergebnisse aus seinem Suchindex, weil diese falsche Tatsachenbehauptungen enthalten und damit rechtswidrig sind. Die umstrittene Funktion „Autovervollständigen“ ist davon – noch – nicht betroffen.

Stärker fiel im ersten Halbjahr 2012 die Steigerungsrate bei den Löschanträgen aus. Google trennt hier zwischen „Urheberrecht“ - zuletzt lag die Zahl der Websites, die wegen solcher Verstöße aus dem Google-Index entfernt werden sollten, bei rund zwei Millionen pro Woche - und „Regierung“. In der Detailansicht wird aufgeschlüsselt nach Verfügungen der Exekutive und richterlichen Urteilen. Während sich seit 2009 die Zahl der Aufforderungen von Regierungen, bestimmte Inhalte zu entfernen, um die tausend Fälle pro Halbjahr bewegte, schnellte die Zahl in den ersten sechs Monaten des Jahres 2012 auf 1791 in die Höhe. Insgesamt 180 richterliche Verfügungen aus Deutschland zählt Google im ersten Halbjahr, 67mal kam die Aufforderung von der Exekutive direkt. 1903 „Inhalte“ sollten entfernt werden. Deutsche Jugendschutzbehörden haben bei Google laut der Selbstauskunft im ersten Halbjahr die Entfernung von 317 Videos beantragt. Bei einer „Mehrzahl“ dieser Videos sei die Anzeige in Deutschland „eingeschränkt“ worden.

Weltweit wollte Microsoft rund 33.000 Domains und mehr als fünf Millionen spezifische URLs in den vergangenen zwölf Monaten aus der Google-Suche entfernen lassen. Auf den weiteren Plätzen folgen die US-und die britische Musikindustrie, NBC Universal, Fox, Sony Music sowie weitere Musik-und Filmrechteverwerter. Nicht enthalten in den Zahlen von Google sind allerdings die Löschanträge für YouTube-Videos. Neben Google veröffentlichen mittlerweile auch Twitter, Dropbox und LinkedIn einen eigenen Transparency Report. Facebook dagegen veröffentlicht weiterhin keine Zahlen zu Anträgen auf Löschungen und Datenherausgabe

(googleblog.blogspot.de/2012/11/transparency-report-government-requests.html; Behörden klopfen öfter bei Google an, www.spiegel.de 13.11.2012; Beuth, Staatliche Überwachung im Netz nimmt weltweit zu, www.zeit.de 14.11.2012).

Weltweit

UN-Bericht fordert mehr Überwachung im Internet

Das UN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) stellte in Wien einen 158-seitigen Report „The use of the Internet for terrorist purposes“ vor, der zu dem Ergebnis kommt, dass Terroristen und andere Kriminelle das Internet nutzen, um Propaganda zu veröffentlichen, Handlanger zu rekrutieren und auszubilden sowie Informationen für illegale Zwecke zu sammeln. Sie machten sich zu Nutze, dass das Internet ein hohes Maß an Anonymität bietet und länderübergreifend funktioniert. Yury Fedotov, Executive Director des UNODC, meinte, genau das mache den Strafverfolgungsbehörden ihre Arbeit so schwer. Der Bericht schildert nicht nur die Gefahren und deren Ursachen, sondern ebenso mögliche Lösungen. Gefordert werden mehr internationale Zusammenarbeit bei der Strafverfolgung und Bekämpfung von Terrorismus sowie mehr Überwachung. Vor allem das Fehlen eines internationalen Abkommens zur Aufbewahrung von Daten sei ein Problem. Die Speicherung von Chats, die etwa bei Skype oder vergleichbaren Diensten tagtäglich geführt werden, könnten zum Beispiel ein probates Mittel zur Verfolgung von Kriminellen sein. Ebenso kritisiert der Report of-

fene WLANs, Videospiele, bei denen der Spieler in die Rolle von Terroristen schlüpft, sowie die Möglichkeiten, soziale Netzwerke, Filesharing-Dienste oder selbst den Index von Suchmaschinen bei der Recherche und der Beschaffung von Informationen für terroristische Zwecke zu missbrauchen (Lanzerath, UN-Bericht fordert mehr Überwachung im Internet, www.welt.de 01.11.2012; der Bericht kann heruntergeladen werden unter

http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf).

Europa

Telefónica verkauft Bewegungsprofile seiner MobilkundInnen

Mit einer Anfang Oktober 2012 eigens dafür gegründeten Abteilung will der Telekommunikationskonzern Telefónica, zu dem auch das kurz zuvor als kleinster der 4 Mobilfunkanbieter in Deutschland an die Börse gehende Unternehmen O2 gehört, als erster Mobilfunkanbieter in Europa die Ortungsdaten seiner KundInnen versilbern. Diese verraten genau, wann und wie lange sich einE KundIn wo aufhält - auch wenn sie nicht telefoniert. Mit solchen Ortungsdaten lassen sich detaillierte Bewegungsprofile erstellen, die Auskunft über Vorlieben, Einstellungen und Gewohnheiten der VerbraucherInnen geben. Diesen Schatz will der Telekommunikationskonzern durch sein Projekt „Telefonica Dynamic Insight“ heben. Grundlage dafür sollte ein neuer unscheinbarer Passus im Vertragswerk des Mobilfunkanbieters sein, wonach z. B. O2 zukünftig nicht nur die Vertragsdaten, also Anschrift, Bankverbindung und Ausweisnummer, sondern auch die bei der Mobilfunknutzung anfallenden Verkehrsdaten zu Vermarktungszwecken nutzen wollte. Zu diesen Daten zählen neben den Nummern der Gesprächspartner auch die Standortdaten der Nutzer.

O2 warb gegenüber seinen Werbekunden mit dem Angebot: „Mit Telefónica Dynamic Insights können Sie ab jetzt sehen, wohin sich Kunden bewegen, während sie sich bewegen. Sie erfahren, wo Ihre potenziellen Kunden wirklich sind, wann sie da sind - und wie oft.“ Ein erster Dienst, bei dem Telefónica mit der Gesellschaft für Konsumforschung (GfK) kooperiert, befindet sich in Großbritannien in der Entwicklungs- und Testphase. Später sollte er auch in Brasilien und Deutschland angeboten werden

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Edgar Wagner kommentierte: „Damit werden unsere Bewegungsprofile wirtschaftlich verwertet!“ Es müsse ausgeschlossen werden, dass höchstpersönliche Informationen meistbietend veräußert werden - dem Supermarkt von nebenan, dem PR-Konzern, vielleicht aber auch dem eigenen Arbeitgeber oder dem misstrauischen Ehegatten. Vor dem „Spion in unserer Hosentasche“ schütze auch keine angebliche „Anonymisierung“ der Daten: Wie ein Geschäftsmodell der Vermarktung von persönlichen Daten ohne jeden Personenbezug funktionieren soll, bleibe völlig unklar. Daher sei Misstrauen angesagt. Wagner forderte die KundInnen auf, schriftlich gegenüber dem O2 Kundenservice, 90345 Nürnberg oder per Mail an kundenerklaerung@o2.com zu protestieren. Die stellvertretende Datenschutzbeauftragte von Schleswig-Holstein Marit Hansen riet verunsicherten MobilfunkkundInnen, sich genau anzusehen, was sie in ihrem Handy-Vertrag unterschreiben. Sollte sich darin ein Passus finden, dass der Übermittlung der Standortdaten zugestimmt werde, so könnte diese Klausel gestrichen oder ihr könnte jederzeit nachträglich widersprochen werden.

Ein Sprecher des für Telekommunikation zuständigen deutschen Wirtschaftsministeriums erklärte am 31.10.2012 in Berlin, Standortdaten dürften nur anonymisiert oder mit Einwilligung des Handybesitzers weitergegeben werden – und dann auch nur an „Dienste mit Zusatznutzen“. Eine Prüfung des Ministeriums habe ergeben, dass die Bestimmungen im Fall O2 einen Handel mit Standortdaten – auch in anonymisierter Form – nicht zulassen, da es sich nicht um einen Dienst mit Zusatznutzen handle. Er gehe davon aus, dass die für die Beaufsichtigung zuständige Bundesnetzagentur entsprechende Schritte einleiten werde.

Die Kritik beeindruckte die Börsenhändler wenig. Das O2-Papier legte einen guten Start hin und stieg am ersten Handelstag von 5,60 Euro auf 5,80. Mit 1,45 Milliarden Euro war dies der größte Börsengang in Deutschland sei Juli 2007 Die spanische Telefónica besitzt nun 77% an ihrer Tochter. Beeindruckt zeigte sich aber Telefónica. Das Unternehmen erklärte nach der massiven Kritik von Datenschutz und Bundeswirtschaftsministerium am 01.11.2012 über einen Sprecher, das Programm „Smart Steps“ werden in Deutschland nun doch nicht verwendet werden: „Datenschutz und Kundenzufriedenheit haben bei Telefónica oberste Priorität. Nach dem Feedback unserer Kunden haben wir uns nun allerdings entschieden, Smart Steps in Deutschland nicht einzuführen“ (PE LfDI Rheinland Pfalz 31.10.2012; Bernau/Paukner/Zydra, Marktforschung mal anders, SZ 31.10.2012/01.11.2012, 19; Bundesregierung: Handel mit Standortdaten grundsätzlich verboten, www.heise.de 31.10.2012; Telefónica: Keine Analyse von Bewegungsdaten in Deutschland, www.heise.de 01.11.2012; O2 stoppt Datenprojekt, SZ 02.11.2012, 19;).

Frankreich

„Oben-ohne-Bilder“ von Prinzgattin Kate untersagt

Ein Richter in Nanterre bei Paris entschied am 18.09.2012, dass das französische Magazin Closer, das die Oben-ohne-Fotos von der Ehefrau Kate des britischen Prinzes William zuerst abdruckte, diese nicht mehr veröffentlichen oder weiterverbreiten darf. Das Magazin wurde zudem dazu verpflichtet, die Originale an die britische Königsfamilie zu übergeben. Die Paparazzi-Fotos zeigen Kate nur mit einem Bikinihöschen bekleidet, wie sie auf der Terrasse eines Privatanwesens in der südfranzösischen Provence in der Sonne liegt oder von ihrem Mann eingecremt wird. Der Herzog und die Herzogin von Cambridge hatten einen Eilantrag bei dem Gericht in Nanterre gestellt, nachdem Closer die

offenbar mit einem Teleobjektiv in ihrem Urlaub in Südfrankreich geschossenen Fotos am Freitag veröffentlicht hatte. In einer einstweiligen Verfügung verbot das Gericht dem Herausgeber des Klatschmagazins, die Fotos „weiterzugeben oder in jedweder Form zu verbreiten", auch im Internet. Die Dateien müssen der Königsfamilie binnen 24 Stunden übergeben werden, für jeden Tag Verzögerung wurde eine Strafe von 10.000 Euro festgelegt. Dem Mondadori-Verlag des früheren italienischen Regierungschefs Silvio Berlusconi, in dem Closer erscheint, wurde von dem Gericht zudem eine Strafe von 10.000 Euro für jeden Verstoß gegen diese Auflagen angedroht. Zudem muss der Verlag 2.000 Euro Gerichtskosten zahlen.

Das Gericht rügte ausdrücklich den „reißerischen" Artikel von Closer. Die Fotos wertete es als ein Eindringen in das Privatleben des Paares. Die Anwältin von Closer, Delphine Pando, hatte argumentiert, dass die Fotorechte nicht der Verlag habe, sondern der Fotograf oder dessen Agentur. Das Magazin habe die Exklusivrechte nur für eine bestimmte Zeit gekauft. Der Antrag von Prinz William und Kate sei daher unzulässig. Closer weigert sich, die Identität des Fotografen preiszugeben. Prinz William und Kate hatten am Tag vor der Gerichtsentscheidung in Nanterre zudem Strafanzeige wegen Verletzung ihrer Privatsphäre erstattet. In diesem Verfahren wollen sie auch Schadenersatz von dem oder den Fotografen sowie von den Verantwortlichen des Magazins erstreiten. Die Staatsanwaltschaft nahm dazu Vorermittlungen auf (Gericht kassiert Fotos von Kate, www.sueddeutsche.de 19.09.2012).

Frankreich

Online-Reputationsversicherung und -management

In Frankreich bieten Versicherungsunternehmen wie Axa und Swiss Life Policen gegen Rufschädigung im Internet an. Die „Protection Familiale Intégrale" hat die französische Axa seit Beginn des Jahres 2012 im Angebot, in Kombination mit einer Versicherung gegen häusliche Unfälle und gegen Naturkatastrophen. Diese Police hilft bei Schädigung der „E-Reputation". Als Beispiele für Versicherungsfälle werden genannt, wenn jemand ungewollt Fotos oder verletzende Äußerungen in sozialen Netzwerken verbreitet, persönliche Informationen oder Kontodaten missbraucht oder wenn es Ärger mit einem Händler nach einem Online-Kauf gibt, etwa weil der die Ware nicht wie beschrieben oder auch gar nicht liefert. Die Versicherung zahlt dann die Anwaltskosten zur Lösung des Streitfalls bis zu einer Summe von 10.000 Euro, bietet einen psychologischen Dienst und zahlt Schadensersatz bis zu 5.000 Euro. Zu dem Paket gehört auch die Bereinigung der „E-Reputation": Unangenehme Daten werden gelöscht und Suchmaschinen-Ergebnisse so manipuliert, dass negative Informationen nicht als Erstes erscheinen. Das Angebot der Axa liegt bei rund 13 Euro monatlich für eine Einzelperson unter 65 Jahren, den Höchstpreis von rund 24 Euro zahlt eine Familie mit mindestens einem Familienmitglied, das älter als 65 ist. Axa Deutschland verfolgt nach eigenen Angaben keine Pläne, eine vergleichbare Versicherung hierzulande einzuführen.

Die Swiss Life bietet in Frankreich seit Sommer 2011 eine ähnliche Versicherung, die laut einem Unternehmenssprecher auf „großes Interesse" stößt. Für einen Beitrag von 9,90 Euro im Monat ist die ganze Familie abgesichert. Swiss Life kooperiert mit Reputation Squad, einer Agentur, die beschädigte Online-Identitäten säubert. Zu ihrer Arbeit gehört auch, vorzeigbare Inhalte über den Geschädigten zu erschaffen, die negative Ergebnisse in einer Google-Suche ausgleichen sollen, wie ein aussagekräftiges Profil in einem beruflichen sozialen Netzwerk wie Xing oder Linkedin.

Auch in Deutschland besteht das in Frankreich versicherte Problem: 42% der Deutschen halten eine solche Police für notwendig, jeder Vierte kann sich gemäß einer repräsentativen Umfrage der Beratungsgesellschaft Faktenkontor grundsätzlich vorstellen, dieses Angebot in Anspruch zu nehmen. Wer hierzulande seine Online-Aktivitäten schützen möchte, kann dies bislang allerdings nur mit einer Internet-Haftpflichtversicherung tun, wie sie zum Beispiel die Allianz oder die HUK-Coburg anbietet. Diese deckt Schäden durch Viren ab oder wenn gegen Persönlichkeitsrechte verstoßen wird, z. B. ein bereits geschützter Domainname abermals angemeldet wird.

Thorsten Rudnik vom Bund der Versicherten meint: „Verbraucher sollten prüfen, ob ihre normale Haftpflichtversicherung auch Aktivitäten im Internet abdeckt, und falls ja, in welchem Ausmaß." Er glaubt, dass der Ruf im Netz heute bedeutender ist denn je. Christian Scherg, Geschäftsführer der Agentur Revolvermänner und Autor des Buchs „Rufmord im Internet" ergänzt: „Meine Reputation im Internet ist genauso wichtig wie mein Lebenslauf. Weil immer mehr Leute ihre Geschäftspartner, Kunden oder andere Kontakte vor dem ersten Treffen oder einem Kauf googeln, sollte man seine Online-Identität gut pflegen." Dazu gehöre, seinen Namen regelmäßig bei Google einzutippen und die Ergebnisse zu überprüfen. Auch empfiehlt er, vorteilhafte Inhalte und Bilder ins Web einzustellen. Jeder könne an seiner digitalen Visitenkarte feilen und Einfluss darauf haben, was online über ihn verbreitet wird.

Ein derartiges Reputationsmanagement wird professionell von Agenturen wie Revolvermänner oder Reputation Squad angeboten. Sie verbessern den virtuellen Ruf von Privatpersonen und Unternehmen, indem sie beispielsweise Negativeinträge korrigieren, löschen lassen oder Profile in Personensuchmaschinen wie Yasni oder sozialen Netzwerken wie Xing veredeln. Zu den Leistungen dieser Agenturen gehört allerdings keine psychologische Hilfe, wie sie die französischen Versicherungen anbieten. Für Christian Scherg ist die Begrenzung des Ersatzes auf 10.000 Euro wenig realistisch: „Bei Rufmord im Internet ist das nichts. Wenn man gegen jemanden im Ausland klagt, wird's schnell sehr teuer." Er hält es für schwierig, die Grenzen zu ziehen: Ab wann muss die Versicherung einspringen? Was ist noch Spaß, was ist schon eine Beleidigung? „Für manche ist ein ins Internet gestelltes Foto in kurzer Hose mit einer Flasche Bier schon Online-Mobbing, andere finden das völlig harmlos" (Pauli, Den guten Ruf im Netz schützen, www.faz.net 17.09.2012).

Belgien

Handy-Affäre im Fall Dutroux

In der seit ihrem Beginn an Justiz- und Polizeipannen reichen Affäre Dutroux ist jetzt der Versuch gescheitert, ein Gespräch zwischen einer Täterin und einem Opfer geheim zu halten. Schuld daran seien angeblich die technischen Tücken eines Smartphones eines der „Vermittler", die am 16.11.2012 dabei saßen, als Jean-Denis Lejeune, Vater eines der Opfer des Vergewaltigers, Kinderschänders und Mörders Marc Dutroux dessen Ex-Ehefrau und Mittäterin Michelle Martin an einem unbekannten Ort traf. Dem Vermittler sei das Smartphone auf den Boden gefallen und aus welchem unglücklichen Zufall auch immer habe das Gerät dann unbemerkt die letzte Nummer der in seiner Anrufliste gespeicherten Gespräche gewählt. Und die gehörte ausgerechnet einem Journalisten der auf der Krawallseite der belgischen Medien angesiedelten SudPresse.

So konnte der Journalist eine Stunde des über dreistündigen Gesprächs mithören und aufnehmen. Nachdem seine Zeitung dann am 17.11.2012 über Inhalte des Gesprächs berichtete, stehen Belgien neue Gerichtsverfahren in der Affäre Dutroux bevor. Die Anwälte von Lejeune und Martin gehen nun gemeinsam gegen den Journalisten und die Veröffentlichung des Mitschnittes vor. Sie haben Beschwerde beim belgischen Journalistenverband eingelegt und gerichtliche Klage eingereicht: Auch in Belgien ist das Abhören eines Gespräches ohne die Einwilligung der Beteiligten strafbar. Georges-Henri Beauthier, der Anwalt von Lejeune, meinte, der Journalist habe die „rote Linie überschritten" (Winter, Fall Dutroux wird zur Handy-Affäre, SZ 19.11.2012, 9)..

Großbritannien

Öffentlichkeitsfahndung nach Steuerflüchtlingen

Die britische Steuerbehörde (HMRC) hat die Namen und Fotos von den 20 meistgesuchten Steuerflüchtlingen des Landes veröffentlicht. Zugleich appellierte die Behörde an die britische Öffentlichkeit, bei der Fahndung zu helfen. Die 20 Verdächtigen werden beschuldigt, aus Großbritannien geflohen zu sein, um der Zahlung mehrerer Millionen Pfund an Steuern zu entgehen. „Um Großbritanniens größte Steuerbetrüger zu fassen, werden wir Fotos der meist gesuchten Betrüger verbreiten", teilte die HMRC mit. Bei den Gesuchten handele es sich um Kriminelle, die nach der Anklage oder während eines Verfahrens untergetaucht seien und die Steuerzahler insgesamt mehr als 765 Millionen Pfund (978 Millionen Euro) gekostet hätten.

Die Regierung sei „absolut entschlossen, gegen Steuerflucht und Steuerbetrug vorzugehen", zitierte die HMRC den britischen Schatzkanzler David Gauke. Mit veröffentlicht wurden Namen, Alter, Staatsangehörigkeit und vermuteter Aufenthaltsort. Einer der dicksten Fische ist der 44jährige Hussain Asad Chohan mit pakistanischer und britischer Staatsangehörigkeit, der u. a. durch Tabakschmuggel dem Fiskus 200 Mio. Pfund (250 Mio. Euro) vorenthalten haben soll.

Die Internet-Aktion reiht sich ein in die Kampagne der britischen Regierung, härter gegen Steuerflüchtlinge und -betrüger vorzugehen. Nach Ansicht von KritikerInnen verhält sich jedoch die Regierung widersprüchlich. Kurz vor der Veröffentlichung der Steuerflüchtlinge warb Premierminister David Cameron um reiche Franzosen, nach London umzuziehen. Ihnen werde an der Themse ein „roter Teppich" ausgerollt". Dies sorgte für Ärger in Paris, wo der französische Staatspräsident Francois Hollande die Einkommenssteuer für Wohlhabende drastisch erhöhen will (Großbrítannien stellt Steuerflüchtlinge bloß, www.zeit.de 16.08.2012; Oldag, Nichts zu lachen, SZ 18./19.08.2012, 26).

Schweden

Datenschutz verhindert Information für Adelsorganisation

Im Jahr 2003 verlor das Ritterhaus (Riddarhusset), die ständische Organisation des schwedischen Adels, seinen Status als öffentlich-rechtliche Körperschaft und wurde, wie jeder einfache Verein, zu einer juristischen Person des Privatrechts. Schon damals erloschen Privilegien der im Riddarhuset vertretenen Adeligen, z. B. mit königlicher Hilfe aus ausländischer Gefangenschaft befreit zu werden. 2012 endet nun als weiteres Vorrecht wegen des Datenschutzes die halbjährliche Information des Ritterhauses durch das schwedische Finanzamt über sämtliche Geburten und Hochzeiten in adeligen Familien. Im Riddarhuset sind 2350 Familien vereint, deren Wappenschilde säuberlich nummeriert im großen Saal des Riddarhus, eines barocken Palastes in der Stockholmer Altstadt, hängen, von Familie Brahe (Nr. 1) bis Zöge von Manteuffel (Nr. 1909). Da die verlässlichen Informationen aus dem Finanzamt ausbleiben, steht die Standesorganisation vor dem Problem, nicht mehr genau zu wissen, wer zum Geschlecht gehört und wer nicht. So könnten aus den Renditen des Vermögens des Riddarhuset (ca. 4,5 Mio. Euro jährlich) nicht mehr rechtssicher Stipendien und Hilfszahlungen an hilfsbedürftige Mitglieder ausgezahlt werden. Von diesen Hilfen profitieren, so Riddarhusets Justiziar Erik Tersmeden, zumeist Witwen und unverheiratete Töchter (Steinfeld, Ein Schlag für die Ritter, SZ 17.10.2012, 1).

Griechenland

Listen mit steuerbetrügenden Reichen werden nur zögerlich genutzt

Evangelos Venizelos, der Chef der griechischen Pasok-Partei, muss der Öffentlichkeit Rechenschaft darüber abgeben, warum er seit August 2011 - damals war er Finanzminister - einen Computerstick mit 1.991 griechischen KundInnen der Genfer Filiale der HSBC-Bank besaß, ohne sich um eine Verfolgung der potenziellen SteuerbetrügerInnen zu bemühen. Der Stick soll zahlreiche Prominente aus Politik, Wirtschaft und Kultur aufführen. Die Gesamtsumme der griechischen Anlagen dieser britischen Bank in der Schweiz beträgt 1,5 Mrd. Euro. Venizelos rechtfertigte sich mit der Aussage: „Elektronische Daten auszuwerten ist nicht meine Aufgabe."

Dies befriedigte jedoch weder seine eigene Partei noch die Mehrheit der GriechInnen, denen zusätzlich zu den bisherigen brutalen Sparmaßnahmen weitere drohen. Venizelos muss sich gegen den Verdacht verteidigen, er habe reiche SteuerbetrügerInnen geschützt, während die Regierung, der die Pasok angehört, die Armen und Schwachen in Bedrängnis bringt.

Die Datei ist auch unter dem Namen „Lagarde-Liste“ bekannt. Christine Lagarde war französische Finanzministerin, als sie 2010 Athen die digitalisierte Kontenliste übergab. Heute ist sie Chefin des Internationalen Währungsfonds (IWF) und entscheidet über dringend benötigte Kredite für Griechenland. Lagarde folgte mit der Weitergabe der Daten einem Wunsch der griechischen Regierung. Finanzminister war damals Giorgos Papakonstantinou, auch ein Sozialist.

In Südfrankreich war zuvor Hervé Falciani, früher Software-Techniker bei der HSBC-Bank in Genf, aufgetaucht. Er hatte Tausende Kundendaten kopiert und wurde in Frankreich wie ein Robin Hood gefeiert, weil Paris mit Hilfe seiner Daten rund eine halbe Milliarde Euro bei französischen Steuerflüchtlingen eintreiben konnte. Auch Deutschland, Spanien und Italien verwendeten die Falciani-Daten und konnten auf dieser Grundlage Milliarden Euro an Steuern eintreiben. Als der französische Staatsanwalt, der Falciani vernahm, in einem Interview davon sprach, dass auch griechische Namen in den Datensätzen zu finden sind, wandte sich Papakonstantinou an Lagarde. Dieser gab an, er habe 10 Namen aussortiert mit KundInnen mit gefüllten Konten, die er dem Chef der Behörde für Wirtschaftskriminalität SDOE übergeben habe. Auf die Frage, warum er nicht alle Namen weitergegeben habe, meinte Papakonstantinou, er habe „kein Vertrauen“ gehabt in die Behörde - für die er selbst damals verantwortlich war.

Der damalige Chef der Finanzpolizei Ioannis Kapeleris behauptete inzwischen in einem Parlamentsausschuss, unter den 10 Genannten hätten sich „keine Politiker und keine namhaften Unternehmer“ befunden. Papakonstantinou wechselte im Sommer 2011 ins Umweltressort und übergab dann die vollständige Liste dem neuen Chef der Finanzpolizei Ioannis Diotis. Dieser meinte gegenüber dem Parlament, für ihn sei die Liste „kein legales Beweismittel“. Er habe den Stick an Venizelos weitergegeben, der ihn in die Schublade seiner Sekretärin legte. Venizelos war 9 Monate lang Finanzminister und verhandelte über Schuldenschnitt, das zweite Rettungspaket und beschwor immer wieder das große Problem der Steuerflucht. Als die Angelegenheit im September 2012 bekannt wurde und der jetzige Finanzminister Giannis Stournaras schon aus Paris eine Kopie anfordern wollte, schickte Venizelos seinen USB-Stick mit Eilkurier an das Büro von Premier Antonis Samaras. Er habe nicht gewusst, „dass niemand außer mir eine Kopie besitzt“. Aus Ärger über Venizelos trat der frühere Innenminister Giannis Ragousis aus der Pasok-Partei aus, der sich u. a. wie folgt erklärte: „Jeder nimmt wichtige Unterlagen aus seiner Dienstzeit mit nach Hause, um sich später verteidigen zu können.“ Inzwischen wird die Liste vom Wirtschaftsstaatsanwalt bearbeitet.

Der Reporter und Verleger Kostas Vaxevanis, der die Liste der Namen mit den HSBC-KundInnen ohne Angaben von Summern veröffentlichte, wurde vor einem Gericht in Athen wegen der illegalen Verwertung persönlicher Daten angeklagt , im Oktober 2012 aber freigesprochen. Er gab zu, dass er nicht wusste, ob die Kontoinhabenden Steuern bezahlt haben oder nicht. Der Staatsanwalt hatte Vaxevanis vorgeworfen „Schuldige und Unschuldige ins Kolosseum des Volkszorns geworfen“ zu haben.

Dies ist nur eine von mehreren Listen, die in Athen kursieren und auf denen Namen von Menschen stehen, deren Vermögensverhältnisse so gar nicht mit dem übereinstimmen, was sie gegenüber den Finanzbehörden angegeben haben. Die größte dieser Listen trägt 54.000 Namen, angeführt von einer Person, deren Initialen „G. D.“ öffentlich genannt werden. G. D. hat ein Jahreseinkommen von 25.000 Euro deklariert, konnte aber 52 Mio. Euro ins Ausland überweisen. Ein anderer auf dieser Liste gab gegenüber der Steuer für das gesamte Jahr 2010 einen Jahresverdienst von 5.588 Euro an, schickte aber 19,8 Mio. Euro ins Ausland. Wieder ein anderer Bürger hatte nach eigenen Angaben exakt null Euro verdient und brachte 9,7 Mio. Euro im Ausland in Sicherheit. Aus Deutschland stammt eine Liste mit 17 KundInnen einer Schweizer Bank. Aus Großbritannien kam eine Datei mit 400 Namen reicher Griechen, die teure Immobilien in London gekauft haben. Wieder auf einer anderen Liste sind die Namen von 20 GriechInnen enthalten, die angeblich Yachten in den Niederladen bauen ließen. Die Finanzbehörden untersuchen auf der Grundlage einer Liste die Vermögensverhältnisse von 60 PolitikerInnen, gegen die nun nicht nur wegen Steuerhinterziehung, sondern auch wegen Korruption, Scheingeschäften und Geldwäsche ermittelt wird.

Der 75jährige Vorsitzende von Transparency International Griechenland Costas Bakouris kommentierte: „Unsere Gesellschaft, so wie sie jetzt ist, ist durch und durch verdorben. Wir sind gierig und unsozial geworden“. In Griechenland seien alle Voraussetzungen für Korruption gegeben: viel Bürokratie, keine funktionierende Justiz, Gesetze mit vielen Schlupflöchern und ökonomischer Druck. Dass all den Informationen auf den Listen jetzt tatsächlich nachgegangen wird, glaubt Bakouris nicht. Der Direktor der Finanzpolizei meinte: „An Listen mangelt es nicht.“ Er habe nicht genügend Leute, um sie zu bearbeiten. Deshalb nennen Vertreter des IWF solche Listen „High hanging fruits“ (Schlötzer/Telloglou, Wertvolle Daten, billige Ausreden, SZ 06./07.10.2012, 10; Heyer, „Durch und durch verdorben“, Der Spiegel 42/2012, 100 f.; Telloglou, Griechische Sitten, SZ 07.11.2012, 26).

Israel

Lügendetektor gegen Geheimnisverrat in Regierung

Der Regierungschef Israels Benjamin Netanjahu drohte der Hälfte seiner Regierungsmitglieder mit dem Einsatz von Lügendetektoren, um einen Geheimnisverrat direkt aus dem Zentrum der Macht aufzuklären. Hinter den fest verschlossenen Türen des Mossad-Hauptquartiers nahe Tel Aviv hatte er sein Sicherheitskabinett zusammengeru-

fen und insbesondere über den Stand des iranischen Atomprogramms informiert. Es ging dabei um nicht weniger als Krieg und Frieden - war also hoch geheim. Doch wenige Stunden nach der Sitzung brachten Medien Details der Debatten ans Licht: Es gebe Streit über das Zeitfenster für einen möglichen Angriff gegen Iran; die Lage würde von vielen als „besorgnis-, aber nicht furchterregend“ eingeschätzt. Diese von Netanjahu und seinem Verteidigungsminister Ehud Barak nicht geteilte Einschätzung führte nicht nur zu einem Folgetreffen des Sicherheitskabinetts, sondern auch zu einer dramatisierten öffentlichen Erklärung: „Die Sicherheit des Staates und seiner Bürger hängt davon ab, dass im Sicherheitskabinett vertrauliche Diskussionen geführt werden können“. Ein Teilnehmer der Runde habe diese grundlegende Regel schändlich verletzt. Deshalb wurden gemäß Presseberichten Yoram Cohen, Chef des Inlandsgeheimdienstes, und Generalstaatsanwalt Yehuda Weinstein beauftragt, gemeinsam zu prüfen, wie die Teilnehmenden an der Sitzung an den Lügendetektor angeschlossen werden können. Netanjahu hatte einen solchen Polygrafen-Test schon im Jahr 2011 nach einer unangenehmen Enthüllung seinen engsten Mitarbeitenden abgenötigt. Der Sicherheitsberater musste anschließend gehen. Die neuerliche Aktion dürfte mit dem Hintergedanken erfolgen, das Sicherheitskabinett zu desavouieren, in dem eine Mehrheit der 14 Minister für einen militärischen Alleingang gegen Iran höchst fraglich ist. Aus dem Lager des Premiers wurde die Bildung eines kleineren Forums erwogen, das die Entscheidungen trifft. Aus diesem handverlesenen Kreis soll dann wohl nur das nach außen dringen, was Netanjahu erlaubt (Münch, Netanjyhu ermittelt, SZ 07.09.2012, 1).

USA

TrapWire: Gefahrendetektion durch anlasslose Verhaltensananlyse

TrapWire ist ein IT-System, das Terroristen und andere Sicherheitsrisiken erkennen soll, bevor die Gefahr sich realisiert. Das zugrunde liegende Konzept heißt Predictive Policing. TrapWire basiert auf bekannten Verfahren der Mustererkennung und von Verhaltensanalysen und gewinnt durch eine starke Vernetzung ein gewaltiges Überwachungspotential. Das System ist inzwischen an vielen Orten vor allem in den USA, aber auch in Großbritannien im Einsatz - in New Yorker U-Bahnen genauso wie in Casinos in Las Vegas, auf öffentlichen Plätzen in San Francisco, rund ums Weiße Haus und an der Londoner Börse.

Quellen der verfügbaren Informationen sind interne E-Mails des amerikanischen Unternehmens Stratfor, das weltweit Bedrohungsanalysen und Einschätzungen zu Konflikten verkauft. Hacker hatten unter dem Namen Anonymous Ende 2011 die Server der Firma angegriffen. Dabei kopierten sie u. a. auch Millionen interne E-Mails, die Wikileaks seit Februar schrittweise veröffentlicht. Die nun bekannt gewordenen E-Mails stammen aus den Jahren 2009 bis 2011, aus denen sich Einzelerkenntnisse über das Überwachungsprogramm ergeben, z. B. ein Kooperationsvertrag, den Stratfor mit der für TrapWire verantwortlichen Firma geschlossen hat. TrapWire ist das Produkt eines Unternehmens namens Abraxas Applications, das heute TrapWire heißt. Da das Unternehmen sein Produkte verkaufen will, gibt es auch öffentliche Äußerungen und Broschüren zu dem Programm. In einem Interview mit dem Firmenchef wird es bereits 2005 beschrieben. Im Fachmagazin Crime&Justice findet sich 2006 eine Vorstellung des Programms. Aus dem gleichen Jahr stammt die öffentlich zugängliche Patentschrift.

TrapWire ist demnach ein Instrument zur Analyse von Videobildern und textbasierten Informationen. Letztere kommen unter anderem von Stratfor. Es soll Auffälligkeiten herausfiltern und vernetzt dazu viele Quellen wie Überwachungskameras und Hotlines.

Da polizeiliche oder geheimdienstliche Bedrohungssituationen von sogenannten Einzelgängern ausgehen, ist man stark zur Aufklärung auf Informationen von Überläufern und aus der technischen (Kommunikations-)Überwachung angewiesen. Da Einzelgänger wenig kommunizieren, sind sie schwer zu finden und können nicht infiltriert werden. Seit Jahren existieren daher Konzepte, die individuelles Verhalten beobachten und so vorherzusagen versuchen, ob jemand einen Anschlag plant. Israel nutzt ein solches Konzept für die Sicherheit des Flughafens „Ben Gurion“. Mit einer Mischung aus Beobachtung und Befragung werden dort potenzielle Täter identifiziert. Gesucht wird nach kleinen Auffälligkeiten, nach bestimmten Verhaltensmustern: unpassender Kleidung, geballten Fäusten, starrem Blick, Nervosität. In Israel übernehmen das ausgebildete Sicherheitsleute.

In den USA geschieht dies automatisiert via TrapWire, wobei die Idee die gleiche ist. Einzelgänger beispielsweise haben niemanden, der ihnen beim Ausspähen eines Zieles hilft. Beobachtet also jemand mehrfach bestimmte Gebäude, vielleicht auch noch auffällig heimlich, kann das bei einem Vergleich von Videobildern auffallen. Ist jemand in einer aufgeregten Menschenmenge ungewöhnlich ruhig, kann auch das einen unguten Grund haben. Die Detektion ist jedoch äußerst schwierig; es kann leicht zu Fehlalarmen komme, zu „false positives“. Die Gründe für ungewöhnliches Verhalten können unterschiedlich sein und sind nur selten Anlass für einen Sicherheitsalarm. Systeme wie TrapWire führen daher leicht dazu, dass sich Unschuldige unangenehme Fragen von Polizisten gefallen lassen müssen.

Möglich ist die Analyse nur, wenn unzählige winzige Informationsschnipsel gesammelt, verknüpft und ausgewertet werden. Das bedeutet, dass jeder Verdacht, jede Spekulation, jede Behauptung für das System relevant sein kann und von TrapWire erfasst werden muss. An vielen Orten in den USA hängen inzwischen Schilder mit dem Satz: „If you see something, say something.“ Damit wirbt das Heimatschutzministerium für „Public Awareness“, also Wachsamkeit der Bevölkerung. Jeder soll bereit sein, Beobachtungen zur Verfügung zu stellen. Online und per Telefon können ungewöhnliche Beobachtungen und Verdächtigungen gemeldet werden. Diese Meldungen von PassantInnen gehen genauso in die Analyse von TrapWire ein wie Berichte von Polizisten über Auffälligkeiten. Eine zweite Quelle sind Videokameras.

Mustererkennungsprogramme suchen in Videobildern z. B. nach parkenden Autos, die immer wieder vor bestimmten Gebäuden stehen. Sie scannen Menschenmengen und können einzelne Personen verfolgen oder auf Wunsch eine ganz bestimmte rote Jacke an verschiedenen Orten wiederfinden. Alle Informationen werden in einer zentralen Datenbank gespeichert und alle Warnmeldungen über Verdächtiges, sogenannte Suspicious activity reports (SARs), werden an die örtliche Polizei und an das Heimatschutzministerium verschickt.

Auch militärische Einrichtungen nutzen TrapWire. Ein Artikel aus dem Jahr 2011 legt die Vermutung nahe, dass mehrere militärische Stützpunkte Tests damit durchführten. In den Stratfor-E-Mails heißt es, dass TrapWire unter anderem auf dem Stützpunkt Fort Meade im Einsatz sei. Das Heimatschutz- und das Verteidigungsministerium haben diverse solcher Verträge mit der Firma geschlossen. TrapWire befindet sich in einer dauernden Weiterentwicklung und Ausweitung. Die Zahl der Beobachtungsquellen wuchs in den vergangenen Jahren genauso wie die Verknüpfungen zwischen ihnen. In einer der E-Mails heißt es, verschiedene Kunden hätten zugestimmt, ihre Daten miteinander zu teilen. So seien alle Casinos in Las Vegas miteinander vernetzt, genau wie verschiedene private und öffentliche Institutionen in Los Angeles.

Die zu beobachtenden Auffälligkeiten beschränken sich nicht auf die Detektion von Terrorismus. In einer von Wikileaks veröffentlichten E-Mail der Stratfor-Mitarbeiterin Anya Alfano an den Vizepräsidenten der Analysefirma Fred Burton, in der es um Sehenswürdigkeiten in San Francisco geht, heißt es: „Sie benötigen so etwas wie TrapWire eher für Bedrohungen durch Aktivisten als durch Terroristen. Für beides ist es sinnvoll, aber Aktivisten gibt es hier viel mehr." Eben solche Aktivisten haben nun eine Googlemap aufgesetzt, auf der sie bekannte Orte von Kameras sammeln, die mit TrapWire verknüpft sind. Sie wollen damit die Aufmerksamkeit darauf lenken, dass die amerikanische Regierung „jeden Bürger wie einen Terroristen behandelt" (Biermann, TrapWire spioniert Bürger in großem Stil aus, www.zeit.de 13.08.2012).

USA

Anlasslose Überwachung im öffentlichen Raum in New York

Das New York Police Department (NYDP) startete ein neues Überwachungssystem mit Nummernschild-Scannern, Kameras und Strahlungssensoren. Der Polizeichef der US-Metropole Raymond Kelly erklärte schon 2010, wie New Yorks Sicherheitsbehörden demnächst arbeiten werden. „Wenn wir nach jemandem in einer roten Jacke suchen, können wir alle roten Jacken der letzten 30 Tage aufrufen." Diese Vision wird jetzt stadtweit realisiert. Das neue Überwachungssystem wurde am 08.08.2012 offiziell eingeweiht. Die Polizei soll damit die Bewegungen aller Personen und aller Autos in der Stadt möglichst vollständig nachvollziehbar machen.

Das System steht, so Bürgermeister Michael Bloomberg, im Dienste der Terrorabwehr, aber auch, „um alltägliche Verbrechen zu bekämpfen." In Manhattan ist das Sicherheitssystem in Teilen schon seit 2007 in Betrieb. Videokameras, Nummernschild-Scanner und Strahlungssensoren überwachen dort den öffentlichen Raum. 3.000 amtliche Kameras gibt es heute in der Stadt, dazu 2.600 Strahlungsdetektoren, mehr als 100 stationäre und dutzende mobile Nummernschild-Scanner. Die meisten Kameras stehen bislang in Manhattan, doch das NYPD hat gemäß dem Bürgermeisterbüro bereits begonnen, „die Kameraüberwachung auf die übrigen Stadtteile auszudehnen". Die riesigen Datenmengen werten die Behörden in Echtzeit aus. Für die Entwicklung des Systems hat sich die Stadt an Microsoft gewandt. New York soll an der Vereinbarung künftig sogar verdienen: Kauft eine andere Stadt die von Microsoft entwickelte Technik, erhält New York 30 % der Einnahmen. Bloomberg bei der Vorstellung der integrierten Überwachungsmaschinerie mit dem Namen „Domain Awareness System" (DAS): „Das ist mehr als nur ein einfaches Dankeschön."

Das System läuft täglich 24 Stunden. Nummernschilder werden gescannt, mit Kameras, die entweder an Tunneln, Straßen, Brücken fest installiert oder aber in Polizeiautos unterwegs sind. Die erfassten Daten werden in das DAS-System eingespeist und abgeglichen, ob sie beispielsweise auf der „Terrorist-Watchlist" auftauchen. Ist dies der Fall, wird die Polizei benachrichtigt: Ort und Zeit der Aufnahme werden gezeigt, zwei Fotos des Autos, ob das Schild schon einmal gescannt wurde, wann das war und welche Nummernschilder in den vorherigen oder darauffolgenden 30 Sekunden noch gescannt wurden. Jessica Tisch, Leiterin der Anti-Terror-Einheit der NYPD, erläutert: „All diese Informationen werden dem Beamten ohne sein Zutun in Sekundenschnelle geliefert." In der Pressemitteilung zum DAS-Start heißt es: „Ermittler können verfolgen, wo ein mit einem Verdächtigen verknüpftes Fahrzeug sich befindet, und wo es sich in den vergangenen Tagen, Wochen oder Monaten befunden hat." Parallel suchen Detektoren permanent nach Quellen erhöhter Strahlung. Das könnte ein Behälter mit Uran oder Plutonium sein - aber auch ein Krebspatient, der gerade von seiner Therapie kommt.

Ein praktisches Beispiel, wie das System funktionieren soll: Eine Kamera informiert die Polizei über eine mögliche Bedrohung. Ein Algorithmus erkennt auf Videobildern, wenn etwa Pakete unbeaufsichtigt vor einem Gebäude abgelegt werden. Ein Polizist setzt sich an den Computer und ruft die Bilder aller Überwachungskameras auf, die sich in einem Radius von 500 Metern befinden. Die Bilder zeigen das Geschehen vor Ort, zu einem beliebigen Zeitpunkt kurz vorher. Ein Blick in die Vergangenheit wird möglich, mit dem man sehen könnte, wer denn das Paket dort abgelegt hat. Die Daten der Nummernschild-Scanner werden fünf Jahre oder länger aufbewahrt, die der Kameras 30 Tage. Bürgermeister Bloomberg erläutert, dass DAS PolizistInnen, ErmittlerInnen und ProgrammiererInnen gemeinsam entwickelt haben, es sei deshalb perfekt auf die Erfordernisse der Beamten abgestimmt und spüle Geld in die Stadtkasse.

In den Richtlinien für das System schon aus dem Jahr 2009 wird immer wieder betont, dass es sich um eine

Maßnahme handele, die explizit gegen den Terrorismus gerichtet sei. Das ganze Dokument argumentiert nach diesem Prinzip und mit dieser Einschränkung. In einer Bewertung kommt die „Michigan Telecommunications and Technology Law Review“ jedoch zu dem Schluss, dass die Richtlinien so schwammig formuliert wurden, dass es ein Leichtes sei, sie für einen beliebigen Einsatz umzudeuten. Zwar solle das System der Terrorabwehr dienen, die Richtlinien sehen aber beispielsweise auch den „zufällig anfallenden Einsatz“ vor, wenn „der Nutzer zufällig etwas bemerkt, das für legitime Zwecke der Strafverfolgung oder der öffentlichen Sicherheit nützlich sein könnte“.

Die Bürgerrechtsorganisation American Civil Liberties Union (ACLU) nennt Nummernschild-Scanner „eine Bedrohung für die Privatsphäre der Amerikaner“. Das größte Problem sei „die Schaffung von Datenbanken mit Ortsinformation über jeden Autofahrer, der dem System begegnet, nicht nur über jene, die die Regierung krimineller Aktivitäten verdächtigt“.

In Deutschland wäre ein solches Vorgehen verfassungswidrig. Das Bundesverfassungsgericht entschied 2012, dass Auto-Kennzeichen nicht generell automatisiert und vor allem ohne Grund erfasst werden dürfen. Doch auch hier findet eine Überwachung von Autokennzeichen, z. B. in Sachsen, wo der Landtag im September 2011 ein Gesetz beschloss, wonach die Polizei zu bestimmten Zwecken Nummernschild-Scanner einsetzen darf. Doch muss der Einsatz zeitlich und räumlich begrenzt werden, wird keine Straftat festgestellt, müssen die Bilder sofort gelöscht werden. Bewegungsbilder von Fahrzeugen zu erstellen, ist explizit untersagt (Tenriverdi, New Yorks Polizei setzt auf Totalüberwachung; www.spiegel.de 10.08.2012).

USA

Online-Gesichtserkennung in der Pornobranche

Unternehmen der Pornoindustrie experimentieren mit Online-Gesichtserkennung. Die Sexplattform Naughty America fordert ihre Kunden auf, Bilder von Frauen bei ihrem „Face“ getauften Onlinedienst hochzuladen. Eine Software sucht dann in den Datenbanken von Naughty America nach Frauen, die denen auf den Fotos ähnlich sehen. Nutzer werden ermuntert, Fotos von Facebook, Instagram oder einer beliebigen Website hochladen. Das Unternehmen SexFaceFinder vergleicht die von seinen Nutzern hochgeladenen Fotos mit denen in einer Datenbank – und zwar der eines Webcam-Dienstes. Beiden Anbietern geht es offiziell darum, dass Männer auf diesem Wege Pornodarstellerinnen finden sollen, die ihren Vorlieben und Fantasien möglichst gut entsprechen.

Die Technik ist noch nicht ausgereift. Das Ausgangsbild und das, was Naughty Americas Gesichtserkennung an Darstellerinnen mit angeblichen Ähnlichkeiten auswirft, stimmen oft nicht überein. Was Naughty America anbietet, wirkt eher wie eine willkürliche Auswahl der eigenen Pornostars. Allerdings bittet der Anbieter um Kommentare, möglicherweise um die Funktion zu verbessern: „Bist du zufrieden mit dem Resultat?“ Wer bei Naughty America ein Bild hochladen will, muss zwar per Checkbox versichern, dass er „das Recht hat, dieses Bild zu verteilen“. Davon dürfte sich aber niemand abschrecken lassen, der gezielt fremde Fotos aussucht. Unklar ist, was Naughty America mit den Bildern macht. Laut Nutzungsbedingungen behält sich das Unternehmen die Weiterverwertung zu allen erdenklichen Zwecken vor. JedeR, von dem es ein Foto im Netz gibt, kann auf diesem Wege so in der Datenbank des Pornoanbieters landen – ohne je davon zu erfahren.

Noch bedenklicher wäre es, wenn ein Anbieter diese Technik einsetzen würde, um eine Datenbank zu durchsuchen, die von den Nutzern selbst gefüllt wurde. Naughty America arbeitet zum Beispiel mit einem Seitensprungportal zusammen. Eine Gesichtserkennung könnte auch die Bilder solcher Portale scannen und damit zum Kontrollwerkzeug etwa für misstrauische Partner werden. Andere Seiten sammeln Nacktbilder, die Menschen von ihren Ex-Partnern hochladen. Was also ursprünglich höchstens ein Mensch sehen sollte, könnte so

für jeden auffindbar werden. Website-Betreiber könnten aus der Rückwärts-Bildersuche ein Geschäftsmodell machen, ohne das Wissen der Betroffenen. Web-Klassiker sind auch Seiten, auf denen „Scherzbolde" die Fotos von fantasievoll dekorierten Betrunkenen veröffentlichen, die im Tiefschlaf nicht mitbekommen, was andere mit ihnen anstellen. Eine Suche mithilfe von Gesichtserkennung erleichtert es, Prominente, Bekannte, potenzielle oder Ex-Partner, Bewerber oder Rivalen auf solche Jugendsünden hin zu überprüfen, vorausgesetzt, die Technik funktioniert irgendwann gut genug. Google bietet bereits eine Rückwärtssuche an, die zum Teil brauchbare Ergebnisse liefert.

Bei Naughty America ist das Angebot vielleicht nur ein billiger Trick, um E-Mail-Adressen sammeln, um diese für Werbung zu verwenden: Wer ein Bild hochlädt, muss nämlich eine E-Mail-Adresse angeben, an die ein Link zum Ergebnis geschickt wird – angeblich wegen des derzeit hohen Suchaufkommens (Beuth, Die Pornoindustrie experimentiert mit Gesichtserkennung, www.zeit.de 21.11.2012).

Technik-Nachrichten

Statistische Auswertung dank Wolfram Alpha für Facebooknutzende

Die Suchmaschine Wolfram Alpha hat für Facebook-Nutzende einen neuen Dienst vorgestellt, mit dem diese über ihre Daten bei dem sozialen Netzwerk bessere Übersicht erhalten. Wozu die Suchmaschine die damit gewonnenen Daten sonst noch nutzt, ist jedoch ungewiss. Der einfach zu bedienende Dienst spuckt binnen Sekunden eine detaillierte Auswertung aller Facebook-Daten aus – mit Tabellen, Tortendiagrammen, Karten und Rankings auf einen Blick: Wie viele meiner Facebook-Freunde sind verheiratet? Welche politischen Ansichten haben meine Kontakte? Wie viele Leute kenne ich in Südamerika? Und welche meiner Fotos und Videos kamen besonders gut an? Je intensiver die Facebook-Nutzung, desto länger und ausführlicher fällt die Übersicht aus. Um den Dienst zu nutzen, muss man in der Suchmaske von Wolfram Alpha „facebook report" eingeben und sich mit einem Facebook-Account anmelden. Wer das tut, erlaubt Wolfram Alpha den Zugriff auf die eigenen Profilinformationen und die seiner Freunde. Diese werden dann durch die semantische Suchmaschine ausgewertet: Heraus kommt ein grafisch aufbereiteter Überblick über die Aktivitäten der NutzerIn und ihrer Kontakte. Auch das Freundschaftsnetzwerk und die eigene Position darin werden angezeigt – gemessen an der Häufigkeit der Kontakte.

Die Suchmaschine Wolfram Alpha, benannt nach ihrem Gründer Stephen Wolfram, ist anders als Google nur zur Beantwortung speziellerer Fragen nützlich, etwa zur Suche nach mathematischen Formeln oder nach anderen spezifischen Fragestellungen. Anstatt eine Liste passender Links zu einem Suchwort auszuschütten, erkennt der Algorithmus von Wolfram Alpha Zusammenhänge und antwortet auf die Suchfrage mit einem konkreten Ergebnis. Bei allgemeinen Fragen klappt das nur begrenzt. Der Suchmaschinen-Betreiber verdient mit Zusatzfunktionen wie dem Facebook-Report, der nur 14 Tage als Testversion kostenlos zur Verfügung steht, sein Geld. Die Pro-Version wird im monatlichen Abo für 4,99 US-Dollar verkauft. Wer das Abo bucht, kann den Statusbericht immer wieder abrufen und aktualisieren. Die Motivation des Suchmaschinen-Entwicklers Stephen Wolfram ist wohl weniger die eines Aufklärers, sondern eher die Faszination über Möglichkeiten der Datenauswertung. Vor einiger Zeit bloggte er einen umfangreichen Text, in dem er seine eigenen Aktivitäten mathematisch analysierte und statistisch aufbereitete. E-Mail, Telefonate, gegangene Schritte – viele Aspekte seines Lebens stellt er darin dar. Viele könnten so etwas, schreibt er nun, denn viele hätten eine sehr umfangreiche Datenquelle zur Hand: Facebook. Wolfram will diese Quelle zugänglich machen. „Wolfram Alpha kennt alle möglichen Informationsquellen. Nun kann es auch Wissen über sie verarbeiten und seine Analysefähigkeiten einsetzen, um diverse persönliche Statistiken zu bieten." Je nachdem, wie die Nutzenden das Angebot annähmen, werde man es in der kommenden Zeit weiterentwickeln, schreibt er.

Was sich dank der veränderten Darstellung plötzlich alles über die eigenen FreundInnen, KollegInnen oder Verwandten offenbart, dürfte die Nutzenden faszinieren. Ihnen sollte jedoch klar sein, dass sie damit zugleich einem weiteren Unternehmen neben Facebook die kompletten Daten aus dem sozialen Netzwerk zur Verfügung stellen. Wie diese in Zukunft verwendet werden, bleibt unbekannt. Voraussichtlich wird die statistische Erfassung und Kategorisierung unseres Lebens in Zukunft immer weiter verbreitet sein. Schon jetzt werden wir von vielen Firmen und Behörden anhand unserer Daten identifiziert und unser Verhalten wird kalkuliert. Data Mining, das Arbeiten in Daten-Bergwerken, ein Art digitale Mustererkennung, ist zu einem mächtigen Werkzeug geworden, bei der Vergabe von Krediten genauso wie bei der Verhandlung um Rabatte. Es gibt eine ganze Szene von Menschen, die ihr Leben als Daten erfassen und auswerten. Bekannt gemacht hat das Konzept der Designer Nicholas Felton, der mehrere Jahre lang sein Leben als grafisch aufbereitete Statistik erhob und veröffentlichte. Er gründete auch eine Website mit, auf der jeder seine Daten sammeln und aufbereiten kann. Inzwischen arbeitet Felton bei Facebook und ist dort

verantwortlich für die Einführung der Timeline, die letztlich eine Sammlung aller Posts einer Person ist. Wolfram Alpha ist ein Versuch, aus diesem Datenstrom Informationen zu gewinnen (Biermann, Erkenne dein Facebook-Selbst mit wolfram Alpha, www.zeit.de 03.09.2012).

Accenture bietet Versicherungs-App „Pay as you drive" an

Das Beratungshaus Accenture hat ein Smartphone-Programm (App) entwickelt, welches das Fahrverhalten von Kraftfahrzeugen (Kfz) misst und die Fahrerbewegungen kontrolliert. Die Daten sollen zur Grundlage für die Kfz-Versicherungsbeiträge genommen werden. Bislang bestimmen vor allem Angaben wie Alter, Wohnort, Fahrzeug, Garage und jährliche Kilometerleistung den jeweiligen Versicherungstarif. Versicherungsunternehmen suchen schon seit längerer Zeit nach Methoden, riskantes Fahrverhalten mit höheren Prämienzahlungen zu belegen. Damit soll zu risikoarmem Fahren animiert werden. Dieses soll belohnt werden und zugleich zum Versicherungswechsel auf dem hart umkämpften Markt anregen. In keiner anderen Versicherungsart werden häufiger die Anbieter gewechselt. „Pay as you drive" (Payd) von Accenture erfasst die gefahrenen Kilometer, die Geschwindigkeit, das Bremsverhalten und die Uhrzeit und leitet diese Daten direkt an den Versicherer weiter. Ist ein Auto besonders häufig nachts unterwegs oder fährt es öfters zu schnell, so kann der Beitrag steigen, bei defensiver Fahrweise kann er sinken. Attraktiv soll das Angebot z. B. für FahranfängerInnen sein, die normalerweise hohe Tarife zahlen müssen.

Verbraucherschützer kritisieren Payd wegen der dauernden vom Versicherungsunternehmen durchgeführten Kontrolle. Es würden sensible Daten erfasst und weitergeleitet. Marit Hansen, stellvertretende Datenschutzbeauftragte von Schleswig-Holstein sieht zudem Schwachstellen bei der Technik: „Apps sind nicht sicher". Die standardisierte Bewertung von Fahrverhalten sei zudem problematisch: „Abruptes Bremsen ist ja nicht per se schlecht. Oft spielen da äußere Umstände eine Rolle." Die Unternehmen erhalten mit dem Verfahren eine exakte Fahranalyse ihrer KundInnen und können möglicherweise direkt auf bestimmte Situationen einwirken. Britische Versicherer haben festgestellt, dass der Schadenaufwand durch Payd-Systeme um bis zu 30% sinken kann, was auf den Kontrolleffekt zurückgeführt wird: Weiß ein Autofahrer, dass er beobachtet wird, fährt er regelmäßig umsichtiger. Erhofft wird durch den ständigen Datenaustausch auch eine engere Kundenbindung. Accenture steht in Verhandlungen mit Anbietern. Eine kurzfristige Anwendung wird angestrebt. Dr. Markus Wensch, Leiter der Versicherungssparte Accenture, meinte: „Ein Breiteneinsatz steht erst noch bevor." Feldversuche hätten eine hohe Zufriedenheit der TestkundInnen ergeben. Die großen Versicherungsunternehmen sind jedoch zurückhaltend. Bernd Engelien, Sprecher der Zürich Versicherung, sieht wegen des Datenschutzes erhebliche Hindernisse. In Branchenkreisen wird gemunkelt, dass praktisch jede große Versicherung eigene Payd-Systeme in der Schublade hat, aber keine den ersten Schritt wagt, so ein Beobachter: „Die Angst vor Ärger mit den Datenschützern und eventuellen Beitragssenkungen ist zu groß" (Freitag, Handelsblatt 01.11.2012).

Schaufensterpuppen beobachten KundInnen

Mehrere führende Mode-Ketten setzen inzwischen Schaufensterpuppen der Firma Almax aus Italien ein, die ihre KundInnen mit Hilfe von Videotechnologie beobachten. In den Augen der Puppen sind Kameras installiert, die mit einer Gesichtserkennungs-Software verbunden sind. Durch das Auslesen der Gesichtsmerkmale kann die Puppe Alter, Geschlecht und Ethnie ihres Gegenübers in Echtzeit erkennen – etwa, ob sich eine junge Asiatin für die Kleidung interessiert. Der Überwachungs-Einsatz soll die Verkäufe steigern. Max Catanese, Geschäftsführer des Herstellers Almax, meinte: „Die gewonnenen Daten dienen Mode-Ketten dazu, ihre Verkäufe zu steigern, indem sie ihre Auslagen besser an das Kundeninteresse anpassen können."

Die 4.000 Euro teuren, sogenannten „EyeSee-Mannequins" hätten beispielsweise in einem Fall herausgefunden, dass über einen bestimmten Eingang überproportional viele Asiaten eine Filiale betreten – und zwar immer nachmittags. Nachforschungen hätten ergeben, dass ein Touristen-Bus in der Nähe des besagten Eingangs hielt. Daraufhin habe der Manager zwei asiatische Verkäufer zu der Zeit im Eingangsbereich platziert – mit dem Ergebnis, dass sich die Verkäufe in der Folgezeit um 12% gesteigert hätten. In einem anderen Laden ergab der Puppen-Einsatz, dass besonders Männer in den ersten beiden Tagen eines Schlussverkaufs zugreifen. Dementsprechend sei die Auslage angepasst worden, um die Verkäufe zu steigern.

Vor allem Modeketten mit großen Filialen setzen die präparierten Puppen nach Herstellerangaben bereits in Europa und den USA ein. Der Wirtschaftsdienst Bloomberg berichtete, dass dazu auch die Benetton-Gruppe gehöre, was ein Benetton-Sprecher aber dementierte. Gemäß Geschäftsführer Catanese soll es auch aus Deutschland Interesse geben, eingesetzt würden die Überwachungspuppen bislang jedoch noch nicht. Seit Dezember 2011 will das Unternehmen mehrere Dutzend Exemplare ausgeliefert haben, noch einmal so viele seien bestellt. Der Puppen-Hersteller verhandelt nach eigenen Angaben derzeit mit mehreren führenden Modeketten über einen flächendeckenden Einsatz. Catanese: „In solchen Läden ist es schwierig, den Überblick über die Kundenströme zu halten." Durch den Einsatz mehrerer Puppen sei es etwa auch möglich, die Verkäufer in Echtzeit dorthin zu lenken, wo ein besonders großer Andrang herrscht. Im Gegensatz zu Videoüberwachungssystemen sei der Vorteil der Puppen, dass sie sich auf Augenhöhe befinden und sich so die Gesichtsdaten detailliert auswerten lassen.

Der Hersteller hat keine Datenschutzbedenken, so Catanese: „Natürlich werden einige Kunden den Gedanken zunächst unangenehm finden, von den Puppen beobachtet zu werden." Doch dazu gebe es keinen Grund. „Wir wer-

den doch ohnehin im öffentlichen Raum permanent beobachtet. Und die Puppen rufen ja nicht meine Freundin an, wenn ich an einem Geschäft vorbei gehe." Die einsetzenden Unternehmen interessierten sich schließlich nicht für individuelle Personen, sondern für verallgemeinerte Daten. Peter Schaar, Bundesbeauftragte für Datenschutz, meinte: „Den Einsatz derartiger Schaufensterpuppen halte ich rechtlich für mehr als zweifelhaft. Auch bei entsprechendem Hinweis wäre solch eine Überwachung kaum zu rechtfertigen." Zusammen mit der „regulären" Videoüberwachung im Geschäft, der Identifizierung beim elektronischen Bezahlen, dem aus der Kundenkarte bekannten Einkaufsverhalten und den aus Funketiketten gewonnenen Erkenntnissen ließen sich mit den Videodaten detaillierte Kundenprofile anlegen. „Eine solche lückenlose Verhaltenskontrolle wäre datenschutzrechtlich unzulässig." Marit Hansen vom Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein kritisierte, dass die Technik auch genutzt werden kann, um unterschiedlichen KundInnen auf einen angeschlossenen Bildschirm verschiedene Angebote zu machen. „Grundsätzlich birgt die Technologie die Gefahr der Diskriminierung - etwa, wenn jungen Asiatinnen plötzlich andere Angebote gemacht werden als europäisch ausschauenden Menschen" (Rest, Modeketten spionieren Kunden aus, www.fr-online.de 21.11.2012).

Hochschuldaten von Hackern aus Protest ins Netz gestellt

Eine Hackergruppe ist in die Server von Dutzenden renommierten Hochschulen eingedrungen und hat Daten ins Netz gestellt. Auch deutsche Hochschulen sind betroffen. Einer Erklärung der Hacker-Gruppe Ghostshell zufolge wollten sie mit ihrer Aktion auf Missstände im Bildungssystem aufmerksam machen. Das „Project Westwind" solle überzogene Studiengebühren in den USA und vorschnelle hochschulpolitische Reformen in Europa anprangern. Zahlreiche amerikanische Elite-Universitäten, darunter Princeton, Harvard und Stanford, sind betroffen, ebenso eine Reihe anderer Hochschulen auf allen Erdteilen. Auch an den Servern von vier deutschen Hochschulen haben sich die Hacker zu schaffen gemacht: die TU Berlin und die Universitäten in Heidelberg, Freiburg und Göttingen.

E-Mail-Adressen, Nutzer-IDs, Passwörter und private Anschriften von Studierenden und Lehrender der Hochschulen wurden ins Netz gestellt. Der Direktor des Freiburger Uni-Rechenzentrums meinte, die Daten seien nichts, was nicht auch per Browser hätte abgefragt werden können. Vertrauliche Informationen seien nicht veröffentlicht worden. Die Gruppe weist in ihrer Mitteilung darauf hin, dass auf den Servern der Hochschulen Hunderttausende weitere Daten offen lagerten. Zudem seien viele der Server mit Schadsoftware verseucht. Der Sicherheits-Dienstleister Identity-Finder analysierte die Schwachstellen der geraubten Daten und stufte sie als authentisch ein. Ein Sprecher des Unternehmens, Aaron Titus, geht davon aus, dass dies keine spontane Aktion war - vielmehr hätten die Hacker mindestens vier Monate gebraucht, um die Daten zusammenzutragen. Das Unternehmen fand mehr als 36.000 E-Mail-Adressen sowie Tausende Usernamen und Passwörter, von denen einige verschlüsselt waren, die meisten jedoch klar lesbar (Hackergruppe stiehlt Daten von Dutzenden Hochschulen, www.sueddeutsche.de 04.10.2012).

Neues zuverlässigere Fingerabdruck-Technik

Ein neues Verfahren aus Israel soll Fingerabdrücke auf Geldscheinen, Verträgen oder Zeitungen, die mit klassischen Methoden nicht mehr sicht- und auswertbar sind, für die Kriminalistik erschließen. Dabei werden nicht die Rillenmuster sichtbar gemacht, die der Fingerschweiß auf Papier hinterlässt; vielmehr wird das unberührte Papier mit Hilfe spezieller Nanoteilchen markiert. So entsteht ein Negativbild des Abdrucks. Ein Forscherteam um Joseph Almog von der Hebrew University in Jerusalem berichtet im Fachblatt „Angewandte Chemie", wie die Methode auch bei schwachen Abdrücken und auf nassem Papier funktioniert. Bisher bringt die Kriminaltechnik Goldnanopartikel auf das Papier, die sich an Aminosäuren in den Schweiß-Resten des Fingerabdrucks heften, was manchmal unzuverlässig ist. Bei der neuen Methode werden Partikel verwendet, die nur auf Papier haften, nicht aber auf Hautfett, womit bessere Ergebnisse erzielt werden können (Wer war´s? SZ 07.11.2012).

Cartoon



Rechtsprechung

EuGH

Österreichische Datenschutzkommission nicht unabhängig

Österreich verstößt gemäß einem am 16.10.2012 ergangenen Urteil des Europäischen Gerichtshofs (EuGH) gegen die EU-Datenschutzrichtlinie (95/46/EG), da die Datenschutzkommission (DSK) organisatorisch zu eng mit dem Bundeskanzleramt verwoben ist. Die Unabhängigkeit sei damit nicht ausreichend gegeben (Az. C-614/10). Bereits der EU-Generalanwalt kam Anfang Juli 2012 zu dem selben Schluss. Kritisiert wird in dem Richterspruch auch, dass der Bundeskanzler sich über alle Gegenstände der Datenschutzkommission informieren kann. Die korrekte Umsetzung der Richtlinie müsse nun „unverzüglich" geschehen. 2003 hatte die Arge Daten Beschwerde erhoben; 2005 rügte die EU-Kommission die Republik Österreich. Es folgte ein jahrelanger Schriftwechsel. Nachdem der EuGH die Bundesrepublik Deutschland 2010 wegen des gleichen Vergehens verurteilt hatte (DANA 2/2010, 85 ff.), klagte die EU-Kommission auch gegen Österreich.

Nach österreichischem Beamtendienstrecht ist der Vorgesetzte „nicht nur befugt, darauf zu achten, dass seine Mitarbeiter ihre dienstlichen Aufgaben gesetzmäßig und (effizient) erfüllen, sondern er hat auch (…) aufgetretene Fehler und Missstände abzustellen, (… und) das dienstliche Fortkommen seiner Mitarbeiter nach Maßgabe ihrer Leistungen zu fördern (...)". Dadurch, so der EuGH, könne die Unabhängigkeit des DSK-Vorsitzenden beeinträchtigt und „vorauseilender Gehorsam" in der Hoffnung auf positive Bewertungen ausgelöst werden. Da die DSK-Mitglieder diese Funktion nur nebenberuflich ausüben, müssen sie „angesichts der Arbeitsbelastung" auf Mitarbeiter zurückgreifen. Diese (wenigen) Beamten sind Mitarbeitende des Bundeskanzleramts und daher ebenfalls nicht unbedingt unabhängig. Es wird bemängelt, dass das geschäftsführende Mitglied der Datenschutzkommission ein der Dienstaufsicht unterliegender Bundesbediensteter ist und dass die Geschäftsstelle der Datenschutzkommission in das Kanzleramt eingegliedert ist. Die genannten Punkte stehen der Annahme entgegen, dass die Datenschutzkommission bei der Erfüllung ihrer Aufgaben jedem mittelbaren Einfluss entzogen ist. Zudem sei die Datenschutzkommission aufgrund dieser Regelungselemente nicht über jeden Verdacht der Parteilichkeit erhaben. Die Klage der Europäischen Kommission als Hüterin der Verträge wurde am 22.12.2010 eingebracht, da sie der Meinung war, Österreich setze die Richtlinie nicht ausreichend um. Mit der Durchführung müsse nach dem Urteilsspruch nun unverzüglich begonnen werden.

Staatssekretär Josef Ostermayer (SPÖ) hat das Urteil „zur Kenntnis" genommen – und wird nach Angaben seiner Sprecherin die nötigen Schritte in die Wege leiten, um den EU-Vorgaben so schnell wie möglich nachzukommen. In der Datenschutzkommission geht man davon aus, dass schon bald rechtliche Anpassungen vorgenommen werden und die Behörde organisatorisch aus dem Bundeskanzleramt ausgegliedert wird. Die Datenschutzkommission steht aber auch aus anderen Gründen vor gröberen Umwälzungen. Ende 2013 soll die Datenschutzkommission nach den Bestimmungen einer Verwaltungsgerichtsbarkeitsnovelle aufgelöst werden. Ob und welche Kompetenzen der Behörde dann den Gerichten übertragen werden, ist noch nicht geklärt. Mit Anfang 2014 wird es jedenfalls eine „Datenschutzbehörde neu" geben. Befugnisse und Organisationsform der neuen Behörde können zudem mit Inkrafttreten der neuen EU-Datenschutz-Grundverordnung neuerlich geändert werden. Die EU-weite Regelung des Datenschutzes plant eine Fülle neuer Aufgaben und Befugnisse für nationale Datenschutzbehörden (Österreich verstößt gegen Datenschutzrichtlinie, futurezone.at 16.10.2012; Sokolov, EuGH: Österreichs Datenschutzbehörde nicht unabhängig genug, 16.10.2012).

BGH

Eltern haften nur eingeschränkt für ihre Kinder online

Eltern haften gemäß einem Urteil des Bundesgerichtshofs vom 15.11.2012 grundsätzlich nicht für das illegale Filesharing eines minderjährigen Kindes, wenn sie das Kind über das Verbot einer rechtswidrigen Teilnahme an Internettauschbörsen belehrt und keine Anhaltspunkte dafür hatten, dass ihr Kind diesem Verbot zuwiderhandelt. In dem zugrunde liegenden Fall klagten Tonträgerhersteller als Inhaber ausschließlicher urheberrechtlicher Nutzungsrechte an zahlreichen Musikaufnahmen. Am 28.01.2007 wurden nach den Ermittlungen eines von den Klägerinnen beauftragten Unternehmens in einer Internettauschbörse unter einer bestimmten IP-Adresse 1.147 Audiodateien zum kostenlosen Herunterladen angeboten. Die Klägerinnen stellten Strafanzeige gegen Unbekannt und teilten der Staatsanwaltschaft die IP-Adresse mit. Nach der im Ermittlungsverfahren eingeholten Auskunft des Internetproviders war die IP-Adresse zur fraglichen Zeit dem Internetanschluss der Beklagten zugewiesen.

Die Beklagten, ein Chefarzt und seine Ehefrau, hatten ihren Internetanschluss auch ihrem damals 13 Jahre alten Sohn zur Verfügung gestellt, dem sie zu seinem 12. Geburtstag den gebrauchten PC des Vaters überlassen hatten. Bei einer vom zuständigen Amtsgericht angeordneten Durchsuchung der Wohnung der Beklagten wurde am 22.08.2007 der PC des Sohnes der

Beklagten beschlagnahmt. Darauf waren die Tauschbörsenprogramme „Morpheus“ und „Bearshare“ installiert; das Symbol des Programms „Bearshare“ war auf dem Desktop des PC zu sehen. Nach Einsichtnahme in die Ermittlungsakte der Staatsanwaltschaft ließen die Klägerinnen die Beklagten durch einen Rechtsanwalt abmahnen und zur Abgabe einer strafbewehrten Unterlassungserklärung auffordern. Die Beklagten gaben die Unterlassungserklärung ab. Sie weigerten sich jedoch, Schadenersatz zu zahlen und die Abmahnkosten zu erstatten.

Die Klägerinnen meinten, die Beklagten seien wegen einer Verletzung ihrer elterlichen Aufsichtspflicht zum Ersatz des Schadens verpflichtet, der durch das unbefugte öffentliche Zugänglichmachen der Musikstücke entstanden sei. Sie nahmen sie wegen des öffentlichen Zugänglichmachens von 15 Musikaufnahmen auf Zahlung von Schadenersatz in Höhe von 200 Euro je Titel, insgesamt also 3.000 Euro nebst Zinsen sowie auf Erstattung von Abmahnkosten in Höhe von 2.380,80 Euro in Anspruch. Das Landgericht (LG) hatte der Klage stattgegeben. Die Berufung der Beklagten beim Oberlandesgericht (OLG) Köln war ohne Erfolg geblieben. Das OLG nahm an, die Beklagten hafteten nach § 832 Abs. 1 BGB für den durch das illegale Filesharing ihres minderjährigen Sohnes entstandenen Schaden, weil sie ihre elterliche Aufsichtspflicht verletzt hätten. Sie hätten die Einhaltung der von ihnen aufgestellten Verhaltensregeln für die Internetnutzung nicht - wie von ihnen behauptet - kontrolliert. Hätten die Beklagte auf dem Computer ihres Sohnes tatsächlich eine Firewall und ein Sicherheitsprogramm installiert, das bezüglich der Installation weiterer Programme auf „keine Zulassung“ gestellt gewesen wäre, hätte ihr Sohn die Filesharing-Software nicht installieren können. Hätte der Vater den PC seines Sohnes monatlich überprüft, hätte er die von seinem Sohn installierten Programme bei einem Blick in die Softwareliste oder auf den Desktop des Computers entdecken müssen. Der Anwalt der Kläger Herbert Geisler plädierte jedoch dafür, dass Eltern ihren Kindern einen Freiraum ermöglichen: „Eltern sollen ihre Kinder zu selbständigem Denken und Handeln erziehen.“

Der BGH hob die Entscheidung des Berufungsgerichts auf und wies die Klage ab. Nach seiner Ansicht genügen Eltern ihrer Aufsichtspflicht über ein normal entwickeltes 13-jähriges Kindes, das ihre grundlegenden Gebote und Verbote befolgt, regelmäßig bereits dadurch, dass sie das Kind über das Verbot einer rechtswidrigen Teilnahme an Internettauschbörsen belehren. Eine Verpflichtung der Eltern, die Nutzung des Internet durch das Kind zu überwachen, den Computer des Kindes zu überprüfen oder dem Kind den Zugang zum Internet (teilweise) zu versperren, bestehe grundsätzlich nicht. Zu derartigen Maßnahmen seien Eltern erst verpflichtet, wenn sie konkrete Anhaltspunkte für eine rechtsverletzende Nutzung des Internetanschlusses durch das Kind hätten. Der Senatsvorsitzende Joachim Bornkamm machte in der Urteilsverkündung deutlich, dass nicht nur die Interessen der Eltern, sondern auch der Unterhaltungskonzerne eine wichtige Rolle spielen. Daraus kann abgeleitet werden, dass, wenn Kinder einmal auffällig geworden sind, strengere Anforderungen gelten. Das Argument, man kenne sich mit der Technik nicht genug aus, dürfte dann nicht mehr vorgebracht werden können (Eltern haften nicht für illegales Filesharing ihrer minderjährigen Kinder, http://www.kostenlose-urteile.de 15.11.2012); Janisch, Risiken und Nebenwirkungen, SZ 16.11.2012, 1, 10).

OLG Hamm

Krankenkasse erhebt illegal Daten bei Minderjährigen

Der 4. Zivilsenat des Oberlandesgerichts (OLG) Hamm hat am 20.09.2012 geurteilt, dass eine Krankenkasse es zu unterlassen hat, ohne Zustimmung der Erziehungsberechtigten bei Gewinnspielen persönliche Daten von minderjährigen VerbraucherInnen ab 15 Jahren zu erheben, um diese als KundInnen werben zu können (Az. I-4 U 85/12). Das OLG änderte damit die erstinstanzliche Entscheidung des Landgerichts Dortmund ab. Die von einer Verbraucherzentrale (VZ) verklagte Krankenkasse hatte auf einer Job-Messe Gewinnspiele für minderjährige VerbraucherInnen angeboten. Auf den Teilnehmerkarten hatte sie Name, Anschrift, Geburtsdatum und Kontaktdaten abgefragt und eine Unterschrift der Teilnehmenden vorgesehen, die nur bei unter 15jährigen Minderjährigen vom Erziehungsberechtigten geleistet werden sollte. Mit einer ebenfalls auf der Karte abgedruckten Erklärung willigten die Teilnehmenden in eine Speicherung und Nutzung der abgefragten Daten ein, um über die Leistungen der Krankenkasse informiert und beraten zu werden. Die verklagte Krankenkasse rechtfertigte ihre Werbung u. a. damit, dass bereits 15jährige Minderjährige ihre Krankenkasse selbst wählen dürften.

Das OLG Hamm widersprach dem und untersagte der Krankenkasse eine derartige Werbung. Es könne nicht davon ausgegangen werden, dass Minderjährige ab dem 15. Lebensjahr grundsätzlich die nötige Reife haben, um die Tragweite der Einwilligungserklärung zur Datenspeicherung und Datenverwendung zu Werbezwecken abzusehen. Zu berücksichtigen sei zwar der mit dem Alter bei Minderjährigen zunehmende Reifeprozess. Abzustellen sei aber auf den Durchschnitt der angesprochenen Personengruppe, die in geschäftlichen Dingen noch unerfahren sei. Beim Lesen der Gewinnkarte überwiege bei ihnen der Anreiz, etwas zu gewinnen, das konsequente Nachdenken darüber, was infolge der Preisgabe der Daten passieren könne. Zudem treffe ein Jugendlicher beim Ausfüllen einer Gewinnkarte auf der Messe eine ganz kurzfristige Entscheidung über die Preisgabe seiner personenbezogenen Daten. Das sei mit der Situation bei der Wahl einer Krankenkasse nicht zu vergleichen. Diese stehe regelmäßig im Zusammenhang mit der Wahl eines Ausbildungs- oder Arbeitsplatzes, bei der ein Jugendlicher von seinen Eltern und ggfls. dem neuen Arbeitgeber beraten werde und sich in Ruhe über die in Betracht zu ziehenden Krankenkassen informieren könne (Oberlandesgericht Hamm: Verbraucherschutz: unzulässige Datenerhebung bei minderjährigen Verbrauchern, PE 09.11.2012).

LG Essen

Internet-Pornografie-Pranger unzulässig

Das Landgericht (LG) Essen erteilte in einem Eilverfahren mit Beschluss vom 26.09.2012 einer bayerischen Kanzlei mit dem Plan eine Absage, die Namen angeblicher Pornokonsumenten, also von Menschen, die beim illegalen Downloaden von Pornografie erwischt wurden, auf ihrer Webseite zu veröffentlichen (Az: 4 O 263/12; s. o. Bayern, S. 171). Die Kanzlei hatte angekündigt, vom 01.09.2012 an eine sogenannte Gegnerliste im Internet zu veröffentlichen. Aufgeführt würden Personen, die illegal pornografische Inhalte heruntergeladen und sich gegen entsprechende Abmahnungen gewehrt haben. Die Kanzlei berief sich dabei auf ein Urteil des Bundesverfassungsgerichts aus dem Jahr 2007, das im Rahmen des Rechts auf freie Berufsausübung Anwälten gestattete, mit einer Veröffentlichung ihrer Gegner zu werben. Die Praxis, solche Gegnerlisten zu veröffentlichen, ist in der Branche inzwischen nicht unüblich.

Neben Privatpersonen sollen auf den Listen der bayerischen Rechtsanwälte auch Pfarrämter, Polizeistationen und Botschaften arabischer Länder auftauchen. Das Gericht entschied, die Mandantin habe zu Recht befürchtet, durch das Erscheinen auf einer Gegnerliste der Kanzlei stigmatisiert zu werden, da öffentlich bekannt sei, dass die Kanzlei auch Anbieter aus der Porno-Branche vertritt. Die Richter bestätigten damit einen Beschluss vom 30.08.2012. Auch nach nochmaliger Prüfung des Sachverhalts blieb das LG Essen bei der Auffassung, dass eine Abwägung der Interessen der Klägerin auf Privatsphäre und der Gefahr der Verletzung der Persönlichkeitsrechte gegen die grundrechtlich ebenfalls bestehenden Interessen der Kanzlei Urmann+Collegen an einer Werbung für sich durch eine Gegnerliste zu Gunsten der Klägerin ausfallen müsse. Anders als bei einer (zulässigen) Gegnerliste, auf der ausschließlich bereits in der Öffentlichkeit stehenden Unternehmen aufgeführt werden, seien die Rechte der Privatperson höher zu bewerten. Jede Privatperson könne sich in seiner selbst gewählten Anonymität bewegen ohne befürchten zu müssen, als Werbemaßnahme öffentlich benannt zu werden.

Es bestehe daher ein vorbeugender Unterlassungsanspruch aufgrund der Ankündigung der Liste ohne klare Festlegung, wer dort erscheinen und wer nicht erscheinen werde. Es sei der Klägerin nicht zuzumuten, abzuwarten, bis der eigene Name veröffentlicht werde, um dann erst dagegen vorgehen zu können. Gerade im Persönlichkeitsrecht sind die Anforderungen an die Begründung einer Erstbegehungsgefahr sehr hoch. Denn für die Zulässigkeit einer Veröffentlichung bedarf es in jedem Einzelfall einer Abwägung zwischen dem Informationsinteresse der Öffentlichkeit und dem Interesse des Betroffenen an dem Schutz seiner Privatsphäre. Eine solche Interessenabwägung kann nur schwer in Bezug auf eine Veröffentlichung vorgenommen werden, die noch gar nicht bekannt ist und bei der insbesondere offen bleibt, mit welchem Inhalt und in welchem Kontext sie getätigt wird. Das bedeutet, dass ein persönlichkeitsrechtlicher Anspruch grundsätzlich nur auf eine Erstbegehungsgefahr gestützt werden kann, wenn der Sachverhalt so gelagert ist, dass praktisch jede Art und Weise der Veröffentlichung rechtswidrig wäre (Lampmann www.lhr-law.de 27.09.2012; Richter verbieten Pornografie-Pranger, www.sueddeutsche.de 26.09.2012).

OVG Rheinland-Pfalz

Hautfarbe als Diskriminierungsmerkmal bei Polizeikontrollen unzulässig

Der Rechtsstreit um die Kontrolle eines Deutschen dunkler Hautfarbe durch Beamte der Bundespolizei ist durch übereinstimmende Erledigungserklärungen der Verfahrensbeteiligten beendet worden, nachdem Vertreter der Bundespolizei sich für die Kontrolle im Zug entschuldigt haben. Dies geht aus einem Beschluss des Oberverwaltungsgerichts (OVG) Rheinland-Pfalz vom 29.10.2012 hervor.

Der Kläger, ein 26-jähriger deutscher Student, wurde im Dezember 2011 auf einer Zugfahrt von Kassel nach Frankfurt am Main von zwei Bundespolizisten angesprochen und aufgefordert, sich auszuweisen, was dieser verweigerte. Daraufhin durchsuchten die Polizisten seinen Rucksack vergeblich nach Ausweispapieren und nahmen ihn mit zu ihrer Dienststelle nach Kassel, wo seine Personalien festgestellt werden konnten. Die Beamten beriefen sich auf eine Vorschrift des Bundespolizeigesetzes, wonach die Bundespolizei zur Verhinderung oder Unterbindung unerlaubter Einreise in das Bundesgebiet in Zügen jede Person kurzfristig anhalten, befragen und von ihr die Aushändigung mitgeführter Ausweispapiere verlangen kann, soweit aufgrund von Lageerkenntnissen oder grenzpolizeilicher Erfahrung anzunehmen ist, dass der Zug zur unerlaubten Einreise genutzt werde.

Mit seiner Klage machte der Kläger geltend, er sei allein wegen seiner dunkleren Hautfarbe kontrolliert worden. Das Verwaltungsgericht (VG) Koblenz hatte zuvor die Klage abgewiesen. Es hatte seine Entscheidung damit begründet, dass der Student auf einer Bahnstrecke unterwegs war, die für unerlaubte Einreisen genutzt werde. Da nur Stichproben möglich seien, dürften Fahrgäste auch nach ihrem Aussehen ausgewählt werden. Die Kontrolle wegen der Hautfarbe erklärte das VG zum „geringfügigen Eingriff“ in das Persönlichkeitsrecht. Die Bundesbeamten hatten ausgesagt, der Kläger sei „aufgrund seiner Hautfarbe ins Raster gefallen“.

Das OVG Rheinland-Pfalz ließ die Berufung zu und vernahm die beiden Bundespolizisten in der mündlichen Verhandlung als Zeugen. Dabei gaben die Beamten nun an, der Kläger habe dadurch Verdacht erweckt, dass er durch den voll besetzten Zug gegangen sei. Nach Beendigung der Beweisaufnahme machte das Gericht deutlich, dass das an den Kläger gerichtete Ausweisverlangen rechtswidrig war, weil die Hautfarbe des Klägers das ausschlaggebende Kriterium für die Ausweiskontrolle gewesen sei. Diese Maßnahme habe daher gegen das Diskriminierungsverbot in Art. 3 Abs. 3 des Grundgesetzes verstoßen. Nachdem sich die Vertreter der Bundespolizei

bei dem Kläger für die Kontrolle im Zug entschuldigt hatten, erklärten die Verfahrensbeteiligten den Rechtsstreit in der Hauptsache für erledigt. Das OVG erklärte das erstinstanzliche Urteil für wirkungslos und legte der Beklagten die Kosten des Verfahrens auf.

Auf die Entscheidung des OVG reagierte Alexander Bosch von Amnesty International mit Erleichterung. Sie sei ein „wichtiges Signal gegen Diskriminierung bei Personenkontrollen. Es ist zugleich eine Genugtuung für all die Menschen, die ähnliche diskriminierende Erfahrungen gemacht haben.“ Die Leiterin der Antidiskriminierungsstelle des Bundes, Christine Lüders betonte, mit dem Beschluss werde eine wichtige Grenze für polizeiliche Tätigkeit gesetzt: „Ich hoffe sehr, dass der Koblenzer Richterspruch jetzt seine Wirkung zeigt.“ Die Deutsche Polizeigewerkschaft erklärte dagegen, der Gerichtsbeschluss sei „schöngeistige Rechtsprechung“, die von der Praxis und ihren Notwendigkeiten keine Ahnung habe (Lenski u. Prantl, SZ 31.10./01.11.2012, 1, 4, 7; www.kostenlose-urteile.de, Racial Profiling: Polizei darf keine Ausweiskontrolle eines Dunkelhäutigen aufgrund der Hautfarbe durchführen).

LAG Hamm

Kein Beweisverwertungsverbot bei fehlendem Vertrauen in Vertraulichkeit

Das Landesarbeitsgericht (LAG) Hamm hat mit Urteil vom 10.07.2012 entschieden, dass das Auswerten des Inhalts von privaten Chatprotokollen für disziplinarische Maßnahmen, hier zur Begründung einer Kündigung, zulässig sei (Az. 14 Sa 1711/10). Die Revision zum Bundesarbeitsgericht (BAG) wurde zugelassen Die Kündigung wurde ausgesprochen, weil der Arbeitnehmer ein gegen ihn gerichtetes Vermögensdelikt begangen haben soll. Zum Beweis wurde auf den Inhalt von Chatprotokollen verwiesen, die der Arbeitgeber auf dem Rechner des Mitarbeiters gefunden hatte.

Das LAG prüfte, ob einer Nutzung der Chatprotokolldaten entgegensteht, dass die Nutzung der privaten Daten des Chatprotokolls gegen das Fernmeldegeheimnis und das Datenschutzrecht verstieß. Es sah zwar eine solche Verletzung als möglich an. Doch leitete es kein Verbot der Verwertung dieser „privaten“ Informationen für den Arbeitgeber ab: Der Beschäftigte müsse damit rechnen, „dass Spuren, die er durch die Nutzung von elektronischen Ressourcen des Arbeitgebers hinterlässt, in einem Prozess gegen ihn verwendet werden“ und zwar, „wenn der Arbeitgeber seinen Arbeitnehmern lediglich eine gelegentliche private Nutzung elektronischer Ressourcen gestattet und zugleich darauf hinweist, dass bei einer Abwicklung persönlicher Angelegenheiten auf elektronischen Geräten und über das Netzwerk der Mitarbeiter keine Vertraulichkeit erwarten und der Arbeitgeber die Nutzung überwachen und bei gegebener Notwendigkeit die Daten einsehen kann“.

Die Fragen zu einem Verwertungsverbots im Bereich datenschutzwidrig erlangter Beweismittel für Arbeitgeber sind bisher nicht eindeutig beantwortet. Das BAG hatte im Juni 2012 im Falle einer Kündigung einer stellvertretenden Filialleiterin einer Einzelhandelsfiliale auf der Basis einer verdeckten Videoüberwachung die Sache an das LAG Köln mit der Begründung zurückverwiesen, dass die „Voraussetzungen für eine prozessuale Verwertung der Videoaufzeichnungen“ zu prüfen seien (DANA 3/2012, 140; Leitsätze: http://www.lag-hamm.nrw.de/service/leitsaetze/index.php; Weigelt www.zeit.de 29.08.2012).

ArbG Augsburg

Beweisverwertungsverbot wegen unverhältnismäßiger Überwachung des Betriebsrats-PCs

Die in Friedberg bei Augsburg ansässige Großbäckerei Ihle verdächtigte einen 54-jährigen Betriebsratsvorsitzenden des Betrugs, ließ seinen PC ausspionieren und kündigte ihn daraufhin. Das Arbeitsgericht Augsburg erklärte diese Spionageaktion mit Urteil vom 04.10.2012 für „nicht verhältnismäßig“ und damit die ausgesprochene Kündigung für unrechtmäßig. Dem Betroffenen war in einer sogenannten Verdachtskündigung vorgeworfen worden, er habe am Rechner des Betriebsrats sein Arbeitszeitkonto zu seinen Gunsten manipuliert. Die Großbäckerei hatte deshalb ohne Wissen des Betriebsrats eine Spähsoftware auf dem Rechner installieren lassen. Die Firmenleitung meinte, so die Rechtmäßigkeit der Kündigung vor Gericht beweisen zu können. Das Gericht wies jedoch den Antrag der Firma Ihle ab, weil die Überwachung des Betriebsratsrechners das „allgemeine Persönlichkeitsrecht von Lothar R. verletzt“ habe und überdies „nicht verhältnismäßig“ gewesen sei, so Manfred Irany, Präsident des Arbeitsgerichts.

In der Begründung machte das Gericht deutlich, dass nur strafbare Handlungen, eine schwere Pflichtverletzung und ein schwerer Vertrauensbruch Grundlage für eine Verdachtskündigung sein könnten. Der Verdacht müsse durch Tatsachen begründet werden und dringend sein. Damit, dass die Firma Ihle auf dem Rechner des Betriebsratsvorsitzenden heimlich eine Überwachungssoftware installiert hat, habe die Firma das Persönlichkeitsrecht des Betriebsratsvorsitzenden verletzt. Sie habe auf mildere Maßnahmen verzichtet und die Kontrolle in einem Übermaß betrieben. Selbst der persönliche E-Mail-Verkehr wurde erfasst. Die sekündlich angefertigten Screenshots erstreckten sich jeweils über eine Dauer von fünf bis sieben Minuten und durften wegen ihrer Unverhältnismäßigkeit im Verfahren nicht gewertet werden. Damit fehlte auch der Nachweis für den von der Firma Ihle angegebenen dringenden Verdacht. Hätte die Bäckereikette nur die Aktivitäten des Betriebsrats auf seinem Arbeitszeitkonto dokumentiert, wäre - so das Gericht - die Überwachung wohl zulässig gewesen, um mögliche Manipulationen nachzuweisen.

Ihle-Personalchefin Jacqueline Dziurla erklärte nach der Urteilsverkündung, man wolle die gerichtlichen Argumente sorgfältig prüfen und erst dann entscheiden, wie es weitergeht. Dabei werde man auch die öffentliche Wirkung des ganzen Verfahrens in die Entscheidung mit einfließen lassen. Die große Aufmerksamkeit, die das Kündigungsverfahren vor dem Arbeitsgericht in den Medien gefun-

den hat, war keine gute Werbung für die Großbäckerei mit ihren knapp 3000 Beschäftigten. Die Gewerkschaft Nahrung-Genuss-Gaststätten (NGG) hatte den Fall publik gemacht. Tim Lubecki, der Geschäftsführer von NGG in Augsburg, forderte die Firma auf, die Kündigung gegen ihren Friedberger Betriebsratsvorsitzenden zurückzunehmen. In diesem Falle sei die Gewerkschaft bereit, mit der Firmenleitung wieder „vertrauensvoll und kooperativ" zusammenzuarbeiten. Die Gewerkschaft hatte zur Urteilsverkündung und für die anschließende Pressekonferenz mit Prof. Wolfgang Däubler von der Universität Bremen einen angesehenen Arbeitsrechtler engagiert, der angesichts der Entscheidung aber nicht mehr viel zu erläutern hatte und sich verbal vor dem Gericht verneigte: „Es gibt noch Richter in Deutschland". Die NGG will eine Strafanzeige gegen Ihle wegen Behinderung der Betriebsratstätigkeit trotz des Urteils aufrecht erhalten, da bisher nicht geklärt wurde, wer die Manipulationen am Rechner des Betriebsratsvorsitzenden vorgenommen hat (Ross, Ihle blitzt vor Gericht ab, SZ 05.10.2012, 34; Bäckerei Ihle: Rechner-Überwachung unzulässig, www.merkur-online.de 04.10.2012; Ihle-Betriebsrat darf bleiben, www.donaukurier.de 04.10.2012).

Buchbesprechung

Hauser, Andrea/Haag, Ina
Datenschutz im Krankenhaus
Deutsche Krankenhaus Verlagsgesellschaft mbH Düsseldorf
4. Aufl. 2012
ISBN 978-3-942734-25-7
372 S., 45 Euro

Die von der Deutschen Krankenhaus Verlagsgesellschaft seit 1990 herausgegebene Veröffentlichung ist mit jeder Auflage umfangreicher und detaillierter geworden. Nach den von Thomas Barta und dann von Jörg Meister und Irene Klöcker inhaltlich verantworteten Vorauflagen haben sich nun zwei Juristinnen mit dem Krankenhausdatenschutz befasst, die als Referentinnen der Rechtsabteilung der Deutschen Krankenhausgesellschaft damit auch beruflich intensiv zu tun haben. Das Buch dient allen, die sich mit dem Datenschutz im Krankenhaus in irgendeiner Weise befassen, als umfassende Informations- wie als Meinungsquelle.

Die Materialsammlung ist einzigartig: Dokumentiert werden alle gesetzlichen Regelungen, die Rechtsprechung und die verschriftlichte Praxis der Datenschutzaufsichtsbehörden von Relevanz. Dabei werden sowohl die ärztliche Schweigepflicht wie auch der Datenschutz mit ihren normativen Wurzeln und in ihrem Wechselspiel dargestellt und an Hand der wichtigsten in der Praxis bisher aufgetretenen Konfliktlagen mit den wesentlichen Argumenten behandelt: Verwaltung, Abrechnung, Organisation, Kommunikation, Datenübermittlung, Dokumentation, Archivierung und Datenvernichtung, Betroffenenrechte, betrieblicher Datenschutzbeauftragter, Forschung… In einem besonderen Kapitel wird der Datenschutz für Krankenhausbedienstete (Beschäftigtendatenschutz) erörtert. Die Präsentation erfolgt in einer gut gegliederten und auch für NichtjuristInnen verständlichen Weise unter vollständiger Angabe aller wesentlichen Quellen (Rechtsprechungs- und Literaturangaben, detaillierte Verzeichnisse zum Inhalt, zu Abkürzungen, zu Stichworten) – auf dem neuesten Stand. Berücksichtigt und teilweise abgedruckt sind die Orientierungshilfe Krankenhausinformationssysteme der Datenschutzbeauftragten des Bundes und der Länder sowie das noch nicht in Kraft getretene Patientenrechtegesetz, ebenso wie alle einschlägigen Spezialregelungen des Bundes (auch im SGB-Bereich) wie der Länder (Landeskrankenhausgesetze).

Das Buch ist aber nicht nur ein hervorragendes Nachschlagewerk, es diskutiert inhaltlich engagiert die behandelten Fragen. Dabei nimmt es durchgängig eine äußerst pragmatische krankenhausfreundliche Position ein, setzt sich aber mit Gegenmeinungen auseinander. So sehr dabei das Anliegen der Funktionstüchtigkeit von Krankenhäusern berechtigt ist, so ist insofern eine kritische Hinterfragung nötig:

Ein beliebtes Legitimationsmuster der Autorinnen ist die konkludente Einwilligung, die sie zwanglos und ohne vertiefte Erörterung der Anforderungen des § 4a BDSG von der Schweigepflicht auf den Datenschutz übertragen. Dabei verwischen sie – aus Darstellungs- und Praktikabilitätsgründen nachvollziehbar, aber rechtlich nicht korrekt – Einwilligung und Vertragsabwicklung. Anstelle des strengen Erforderlichkeitsgrundsatzes wird der weniger verbindliche Verhältnismäßigkeitsgrundsatz bemüht (etwa bei Zugriffsbeschränkungen, S. 50). Bei der Darstellung der Auskunfts- und Einsichtsrechte der PatientInnen wird zwar die moderne Rechtsprechung referiert, aber zugleich auf die entschiedenen Fallgestaltungen beschränkt, so dass rechtlich völlig überholte und äußerst fragwürdige Einschränkungen des Auskunftsrechts (z. B. die auf objektive Befunde, S. 63, im Hinblick auf Infektionsberichte, S. 71) vorgetragen und vertreten werden.

Überpragmatisch ist auch der Umgang mit dem Dilemma der praktischen Notwendigkeit des Outsourcing einerseits und der Wahrung des Patientengeheimnisses andererseits. Hier den Medizinprodukteberater bei der Operation (S. 52), den fernwartenden externen Systemadministrator (S. 109) bzw. den Auftragsdatenverarbeiter generell (S. 108) als berufsmäßig tätigen Gehilfen und als rechtmäßigen Verarbeiter von Patientengeheimnissen einzustufen, ist zwar vom Ergebnis für das Krankenhaus her bequem, entspricht aber nicht ei-

ner sauberen rechtlichen Ableitung noch der herrschenden Meinung in Rechtsprechung, Literatur und Aufsicht.

Äußerst erfreulich ist die ausführliche Behandlung der mit der Abrechnung verbundenen Datenschutzfragen, sowohl im Hinblick auf die Krankenkassen und die gesetzliche Krankenversicherung wie auch hinsichtlich der privatärztlichen Abrechnung. Bezüglich der Datenweitergabe an private Versicherungen wird zwar der zentrale Beschluss des Bundesverfassungsgerichts von 2006 referiert, nicht aber die Konsequenz hieraus in Form von Musterformulierung von Schweigepflichtentbindungserklärungen, auf die sich die Datenschutzaufsichtsbehörden mit dem Gesamtverband der Deutschen Versicherungswirtschaft geeinigt haben (http://www.datenschutz.hessen.de/dk20120117.htm). Diese kleineren Mängel ändern aber nichts am Gesamturteil: Wer mit Datenschutz im Krankenhaus zu tun hat, für den ist dieses Buch Pflichtlektüre; ja für die meisten Fragestellungen genügt es sogar als einzige Informationsquelle. Es geht (soweit eine widerspruchsfreie Argumentation dies erlaubt) rechtlich in die Tiefe und gibt den PraktikerInnenvor Ort Hunderte von direkt anwendbaren nützlichen Tipps.

Mitmach-Aktion des Landesverbandes der Humanistischen Union Baden-Württemberg

Musterbrief

Adresse Datum

Anschrift

Betr.: Lichtbildanforderung für die elektronische Gesundheitskarte

Sehr geehrte Damen und Herren,

Sie haben mich gebeten, Ihnen mein Lichtbild für die Anfertigung der elektronischen Gesundheitskarte zu übersenden. Gegen diese Lichtbildanforderung lege ich hiermit

Widerspruch

und begründe diesen nachfolgend:

Zunächst halte ich es für grundsätzlich unnötig, dass meine eGK mit meinem Foto versehen wird. Mein Arzt und meine Ärztin kennen mich in Person. Wer mich nicht kennt, kann sich meiner Identität zusätzlich durch einen Blick in meinen Personalausweis und dortiges Foto vergewissern. Ein Foto in der eGK ist also gar nicht notwendig.

Unabhängig davon halte ich es auch aus nachfolgend dargestellten rechtlichen Gründen für unzulässig, von mir ein Foto zu Einstellung in die eGK zu verlangen:

Die Anforderung des Lichtbildes stellt einen Verwaltungsakt dar, da in dem Schreiben – in Fettdruck hervorgehoben – auf die gesetzlich verankerte Pflicht der Versicherten zur Lichtbildbereitstellung hingewiesen wird. Da Ihr Aufforderungsschreiben dazu dient, die öffentlich-rechtliche Regelung in § 291 SGB V umzusetzen, liegt ungeachtet der äußeren Form des Schreibens ein öffentlich-rechtliches Handeln vor. Das Schreiben entfaltet für den Adressaten auch belastende Wirkung, da dieser ein Lichtbild anfertigen lassen muss und es anschließend übersenden muss.

Die Lichtbildanforderung ist nach hier vertretener Auffassung rechtswidrig. § 291 SGB V verlangt, dass auf der Krankenversichertenkarte „Lichtbild und Unterschrift des Versicherten“ aufgebracht werden. Sinn dieser Regelung ist es, Missbräuche dadurch zu verhindern, dass die eGK mittels Lichtbild und Unterschrift ähnlich dem Personalausweis oder Reisepass zu einem Ausweis- und Identifikationsdokument ausgestaltet wird. Dies ergibt sich auch klar aus Anlage 4a des BMV-Ä. Dort heißt es in Anhang 1 unter Ziffer 1.2.:

„Der Arzt ist verpflichtet, die Identität des Versicherten zu prüfen. ... Die Identität des Versicherten ist anhand der auf der elektronischen Gesundheitskarte aufgebrachten Identitätsdaten (Lichtbild, Unterschrift, Name, Vorname, Geburtsdatum) zu prüfen.“

Eine solche Identitätsprüfung durch den Arzt ist aber nur möglich, wenn bereits bei der Herstellung der eGK ein identitätsgeprüftes Lichtbild verwendet worden ist. Ich verweise ergänzend auf eine im Internet veröffentlichte Broschüre des BMG mit der Bezeichnung „Die elektronische Gesundheitskarte“. Dort heißt es auf Seite 10: „Das aufgedruckte Foto weist einen Versicherten zweifelsfrei als Inhaberin oder Inhaber der Karte aus.“ Auch hat das BMG durch die damalige Frau Staatssekretärin Caspers-Merk (Lörrach) auf eine Bundestagsanfrage mit der Arbeitsnummer 11/75, die die Notwendigkeit einer Identitätsprüfung durch die Krankenkassen bei Ausgabe der eGK betraf, im November 2008 dahingehend Stellung genommen, dass zwar die Ausgestaltung des Verfahrens in der Zuständigkeit der Krankenkassen liege, dabei aber Verfahren zu bevorzugen seien, die eine Identitätsprüfung der Versicherten beinhalten.

Ohne eine solche Prüfung wird es weiterhin Missbräuche gerade durch jene Personen geben, die auch bisher schon in betrügerischer Weise zum Schaden der Versicherten Leistungen der Krankenkasse erschlichen haben. Solange in dem Verfahren zur Ausgabe der eGK nicht sichergestellt ist, dass die eGKs auch tatsächlich mit einem Foto des Karteninhabers versandt werden, kann die eGK ihre gesetzlich vorgesehene Funktion nicht erfüllen. Insbesondere wäre es nicht möglich, die eGK in der im BMV-Ä vorgesehenen Art und Weise zu verwenden.

Mit freundlichen Grüßen


Es war einmal...
Ihr Internet-Browser versucht gerade, Kontakt zu einer Webseite herzustellen, die im Zusammenhang mit der Verbreitung von Kinderpornografie genutzt wird. Kinderpornografie stellt sexuelle Missbrauchshandlungen an Kindern dar. Die Verbreitung, der Erwerb und der Besitz von kinderpornografie ist nach § 184 b Strafgesetzbuch strafbar.
Der sexuelle Missbrauch von Kindern bedeutet für die Opfer das Erleiden physischer und psychischer Gewalt und ist in der Regel mit lebenslangen Schädigungen verbunden. Durch die Dokumentation und Veröffentlichung der Taten im Internet werden die Opfer zusätzlich traumatisiert und dauerhaft in der Öffentlichkeit stigmatisiert. Zudem generiert die massenweise Verbreitung im Internet die Nachfrage nach neuem Material und fördert so zumindest mittelbar die Begehung weiterer Missbrauchstaten.
STOPP!
Falls Sie Einwände gegen die Sperrung dieser Webseite haben oder sie für nicht korrekt oder ungerechtfertigt halten, so kontaktieren Sie bitte das Bundeskriminalamt unter folgender E-Mail-Adresse kontakt@bka.de.
Weder Informationen zu Ihrer IP-Adresse noch andere Daten, anhand derer Sie identifiziert werden könnten, werden vom Bundeskriminalamt gespeichert, wenn diese Seite erscheint. Die Sperrung dieser Webseiten erfolgt ausschließlich, um die kriminelle Verbreitung von Darstellungen sexuellen Missbrauchs und die weitere Ausbeutung der Kinder zu erschweren.
Die Suche nach Kinderpornografie und die Beweissicherung ist ausschließlich Sache der Polizei.